TO BE APPROVED AT THE NEXT REGULARLY SCHEDULED COMMITTEE MEETING

Risk Management Committee

October 22, 2020
9:30 A.M.

Attendees: Dick Boccaccio, Marjorie Lemmon, Mike McCormack, Chris Poulos, Mark Raymond, Jeff Brown, Fred Tanguay, Doreen Lessard, Richard Poirier, and Eileen McNeil.

1. Call to Order

   Mr. Poulos called the meeting to order at 9:32 A.M.

2. Minutes of Meeting held on September 10, 2019 – Approval

   It was not necessary to approve the minutes from the meeting held on September 10, 2019 since there was not a quorum at that meeting. The committee requested a copy of the minutes from the previous Risk Management Committee meeting held on April 23, 2019.

3. Chairman's Vision and Charge to Committee Members

   The committee members reviewed the vision and charge prepared by Mr. Poulos and had no comments.

4. Written Report from DAS Fleet Operations (Russ Wininger)

   The committee reviewed the report provided by Mr. Wininger noting the high number of accidents for the Department of Correction and DCF. Mr. Tanguay advised that Fleet Operations is in process of trying to get funding to implement telematics. Telematics includes a GPS type device installed on vehicles that can not only track the vehicles location, but can also track speed, hard braking, idling etc.

   Mr. Poulos advised that he will request that Mr. Wininger provide a year-to-date report for 2020 for the next committee meeting.

5. Report from DAS Information Technology (Mark Raymond, Jeff Brown) on status of Cyber Liability/Security

   Mr. Raymond explained that there are two major data centers that the majority of agencies use. Some agencies (DOT, Labor Department, Department of Correction, and Chief Medical Examiner) have their own data centers. Agencies are starting to move to cloud-based services and application based services and there is more complexity to secure cloud-based data. Mr. Raymond noted that DAS has a large collection of fiscal, personal and health information data and the cyber security risk is in the access and protection of this data. His office has worked with OPM to submit a State data plan in 2018. A refresh plan will be submitted this year. This plan can be found on OPM's website. He stated that there are 748 different data sources managed by the state and out of those, 363 contain protected and/or federally restricted data that is not available to the public. 311 data sources can be shared with the public. The goal is to track the information we have and try and protect it. Mr. Raymond explained that the trend is going toward more digital government which provide more 24/7 on-line services but also opens the opportunity for fraud. The more that is available on-line, the more security is needed to prevent fraud.

Mr. Raymond explained that DAS is constantly updating its Cyber Security Action Plan. Each administration has a slightly different approach. He also stated that DAS has an Incident Response Plan which is followed if an agency has a cyber security incident. DAS also has a Disruption Response Plan which addresses statewide disruption and has conducted table top exercises of this plan. He advised that there is a Cyber Security Committee which meets monthly and consists of State, local and private members. The committee recently helped the City of Hartford with its ransomware attack.

Mr. Raymond advised that DAS recently entered into an agreement with Microsoft which provides updates to the operating system and that all email has been moved to the cloud. Upon a question from Mr. Poulos, Mr. Raymond stated that there is a $24 billion aggregate exposure to the State as a whole (total State annual revenues) and little cyber insurance in place except for some of the colleges. He noted that in the cloud-based agreements all have cyber insurance requirements with them also having indemnity requirements.

Mr. Raymond stated that when the COVID pandemic first hit, most State employees started to work from home within a three week period. DAS went from 2,000 VPN connections to over 10,000 VPN connections. He noted that with the huge uptick of a work-from-home environment in a short period of time, there was more complexity in getting all the computers secure and his staff was working round the clock.

Mr. Raymond said that some activities that were put in place before COVID had to be put on hold such as IT optimization. The goal is getting all IT services centralized, adding more 24/7 monitoring, addressing where the vulnerabilities are and finding ways to correct them.

Mr. Poulos asked what the highest exposure the State would incur. Mr. Raymond estimated that the worst case scenario would be that the Personal Identifiable Information of 3.4 million people would be lost and would cost the State approximately $800 million a year for two years to provide credit protection.

Mr. Tanguay asked Mr. Brown who previously worked for AIG, if he sees a value in the State purchasing more cyber liability insurance. Mr. Brown advised that it makes sense for a smaller entity, but possibly not for the State since the State has various systems in place.

Mr. Poulos thanked Mr. Raymond and Mr. Brown for its presentation to the committee.

Mr. Poulos went on to say that he reached out to the Risk Management Departments in four states, Oklahoma, Florida, Kentucky and North Carolina to see how they address cyber liability. Mr. Tanguay will give the STRIMA website to Mr. Poulos so that he can post his question on the website. Mr. Tanguay noted that approximately 30 states are active in the STRIMA association.

6. Other Matters to Come Before the Committee

There were none.

7. Next Meeting – Date and Location

   The 2021 Risk Management Committee meetings will be set once the Board meeting dates are set. Mr. Poulos would like the committee meetings to be held three or four weeks prior to the Board meetings.

8. Motion to Adjourn

   A motion was made by Mr. Boccaccio, seconded by Mr. McCormack and unanimously

   VOTED: The meeting be adjourned. The meeting adjourned at 10:57 A.M.