



## Delaware Cyber Security Advisory Council

09/10/2019 09:00 AM

Public Service Commission Conference Room, 861  
Silver Lake Blvd., Dover, DE 19904

### Meeting Minutes

Printed : 1/2/2020 11:41 AM EST

#### Delaware Cyber Security Advisory Council (CSAC) Mission Statement

The Delaware Cyber Security Advisory Council is a cross-sector group that explores and promotes best practices to prepare for and prevent cyber security events, makes collaborative recommendations for effective response to such events, and makes recommendations regarding training and resources necessary to drive a culture of cyber preparedness to the citizens, businesses, and organizations that live and operate in the State of Delaware.

**Location:**  
Blvd., Dover, DE 19904

Public Service Commission Conference Room, 861 Silver Lake

**Type of Meeting:**

CSAC Meeting

**Meeting Facilitator:**

CIO James Collins

#### Attendees

##### Present Committee Members

James Collins	Department of Technology and Information (DTI)
Solomon Adote	Department of Technology and Information (DTI)
AJ Schall	DEMA
David Bell	Exelon
Michael Hojnicky	New Castle County Government
Joshua Bushweller	Delaware State Police
Jason Christman	Delaware National Guard
Richard Gowen	Verizon
Marwan Rasamny	Delaware State University

##### Also Present

Claudette Martin-Wus	DTI
Sandee Alexander	DTI
Shelley Turner	DTI
James Robb	City of Wilmington
Trevor Fulmer	JP Morgan Chase
Lisa Morris	Department of Justice
Jon Bell	Delaware Better Business Bureau

## I. Welcome and Introductions

The meeting commenced at 9:02 a.m.

## II. Review and Approval of Last Meeting Minutes

- a. The committee reviewed the Committee Meeting minutes from June 19, 2019.
- b. Committee members had no revisions or comments. AJ Schall made the motion to accept the minutes and J. Christman seconded. The motion was approved.

## III. Chairperson Update

- a. J. Collins current President of NASCIO informed the committee that NASCIO has issued some guidance for local governments on things that they can do to help prevent ransomware attacks. NASCIO has endorsed some federal legislation supporting local governments. As local governments, school districts and the private sector seem to be the target of these ransomware attacks.
- b. J. Collins and S. Adote are working with M. Hojnicky and C. Luft (local government) to better identify and reduce the risk of future attacks. They asked that this be an agenda item at the next DCSAC meeting.
- c. M. Rasamny suggested that the council start thinking about shared services, so that everyone can contribute – possibly form a taskforce.
- d. J. Collins recommended a secure platform in support of M. Rasamny's recommendation of shared services. Legislation was passed to centralize IT services across the state. There needs to be a conversation with the decision makers to ensure that they are leveraging IT services.

## IV. State of Local Government

- a. M. Hojnicky shared a list of tools and services provided by MS-ISAC to the State and local governments. Most of these tools are free of charge and provide a host of services which are in the best interest of our state and local government. One of the services provided is a weekly report listing known IP addresses being shared on the dark web. At this time their primary focus is on the upcoming elections, but if requested they will perform a vulnerability assessment.
- b. Tools provided by MS-ISAC are:
  1. NCSR – A self-assessment identifying your strengths and weaknesses
  2. Secure Suite Member – Allows members to use tools on how to harden information.
  3. M-cap – Allow you to submit emails to identify risk you have averted.
  4. The Albert Tool – This is a tool that has been used by DTI in the past.
- c. J. Collins requested that the role of the National Guard be better defined.
- d. J. Christman explained that the National Guard would have to be tasked and a conversation to explore the needs would than need to occur. Once the National Guard has been activated rapid response can be taken on.
- e. J. Collins pointed out that if we can get to the point of assessment coupled with strategy, we can than help mitigate the risk to the private sector and local government. A subcommittee can be put together to conduct that business. This committee can form a subcommittee for this task.
- f. AJ Schall noted that there are hundreds of thousands of dollars go into cyber security each year and that this is a discussion to have during a DEMA-held grant meeting.

g. S. Alexander provided information on Securing the Human training which is purchased through a grant. Joe Hughes is the contact person for obtaining grant funds through the DEMA Training and Exercise Subcommittee for Local Government.

## **V. Cyber Trends - Cyber Security Awareness Month (CSAM) Activities**

a. S. Alexander provided details regarding the upcoming Secure Delaware event being held at the Chase Center in Wilmington, Delaware on September 24, 2019. This year's presentations focus on small businesses.

b. Secure Delaware sponsors for this year included:

1. Splunk
2. Wilmington University
3. Microsoft
4. Cisco; and many more

c. J. Collins added that this event is not just a techie event, it's about mitigating risk.

d. We are trying to get as much safety and security information out as possible to help better protect the state. The DigiKnow website is for the public to educate and raise the cyber security posture.

e. H. Volkomer asked that committee members take copies of the flyers for the 4th grade presentations and distribute them at their local schools.

## **VI. Strategic Planning Activity for Revised Council Objective**

A. Review results from previous strategic planning activity

a. This committee can form subgroups.

b. DTI has worked with DEMA in the past. We need to continue to leverage those opportunities.

c. S. Alexander suggested that tabletop exercises be a standing agenda item for the committee rather than assigning it to a subcommittee.

d. S. Adote added that "who to call first" when a cyber event occurs needs to be part of our regular meetings.

e. J. Collins suggested that instead of participating in a tabletop exercise this committee should host a tabletop exercise. It would be focused on local government agencies and small businesses. Rollout a webinar focusing on small business and local government. Start off with lessons learned then move people into the exercise.

f. G. Schoenberg explained that this would be considered a multi-disciplinary team and that there are already a lot of free resources being offered through Department of Justice (DOJ).

g. S. Alexander suggested that we use social media to take advantage of microlearning opportunities – everyday help aides in learning.

h. J. Bell added that a phishing tool could also be used as an opportunity.

i. M. Rasamny stressed the important role citizen play. They are part of our critical

infrastructure.

j. J. Collins stated that upcoming sessions would include discussions about webinars and microlearning for citizens. We also need to figure out how to share threat information amongst our own agencies.

k. Representatives from the DIAC were asked to investigate how more mature agencies are doing this as well as develop recommendations on how to expand sharing threat information. Private sessions may be needed to achieve this goal.

l. J. Bushweller of the DIAC agreed to look into this request as this would be an excellent opportunity to fill some of the gaps. The DIAC will have a full-time analyst dedicated to cyber security.

m. M. Hojnicky reminded committee members of the upcoming budget and that this committee should support the DIAC in their need for an analyst for cyber security.

n. J. Collins added that the Governor is a strong proponent of public/private partnerships. There were discussions about forming a Delaware ISAC.

o. J. Christman clarified that some threat information may not be related to the citizens but to the critical processes that the citizens use and that you may not need to notify citizens because of sensitive information.

p. At the request of J. Collins, J. Christman agreed to work with the DIAC regarding information sharing.

B. Determine Leads for each Subcommittee and recruitment of members

N/A - this agenda item was not needed based on previous discussion during the meeting

C. Determine schedule for Threat Info Subcommittee schedule

N/A - this agenda item was not needed based on previous discussion during the meeting

## **VII. New Business**

a. Discuss third party supplier risk.

b. Discussion for a future meeting will be Capital One breach and 3rd party suppliers, Colorado Transportation breach, MS-ISAC resources and how JP Morgan Chase is dealing with some of these issues.

c. J. Collins clarified that when leveraging infrastructure all security controls are still our responsibility.

## **VIII. Surveys**

Survey agenda item discussed during Public Comments.

## **IX. Public Comment**

a. J. Bell with Delaware Better Business Bureau regarding the most recent Cyber security breach. The Delaware Better Business Bureau sponsor presentations educating Public / small businesses but be aware that people will not take advantage of this opportunity without some type of incentive. They would be interested in sharing their experiences.

- b. At the request of J. Collins, J. Bell agreed to share his contact information with the group.
- c. C. Martin-Wus had composed surveys attached to the agenda. The exercise survey is the one needed to be filled out and will be emailed to committee members.

**X. Old Business**

None

**XI. Adjourn**

J. Collins thanked all attendees. The meeting was adjourned at 11:02 a.m.

---

-

---

-