ARIZONA CYBERSECURITY TEAM
MINUTES

October 4, 2018
9:00 AM
1700 West Washington Street,
Governor's 2nd Floor Conference Room
Phoenix, Arizona 85007

A meeting of the Arizona Cybersecurity Team (ACT) was convened on March 26, 2018 at 9:00 AM in the 2nd Floor Conference Room, 1700 West Washington, Phoenix, Arizona 85007. Notice having been duly given. Present and absent were the following members of the Council:

Members Present	
Mike Lettman (Co-Chairperson)	Frank Milstead
Frank Grimmelmann (Co-Chairperson)	Martin Hellmer
Tim Roemer	Kathleen Fernandez
Morgan Reed	Austin Kennedy
Gil Orrantia	Christine Figueroa
Michael McGuire	Tina Slankas
Sandra Watson	Brian Mueller
Jason Isaak	Dane Mullenix
Linda Medler	

Members Absent
Shay Stautz
David Boynton
Jon Haass
Jeff Weninger
Michele Reagan
Bob Worsley

Staff Present
Megan Fitzgerald

1. CALL TO ORDER

Mr. Mike Lettman called the meeting to order at 9:10 AM.

2. INTRODUCTIONS

Mr. Tim Roemer gave opening remarks and welcomed those in attendance on behalf of Governor Ducey.

Mr. Roemer thanked all of the members of our Arizona Cybersecurity Team for attending. The Governor created this team due to increasing threats in the realm of cybersecurity. Arizona is a leader in cyberspace and cyber education, but we must continue to work together to do better. Breaking down silos and sharing information across a variety of sectors is a great first step. This team was created not only to look for best practices but to analyze what practices will work best for Arizona. Cybersecurity and cyberspace is a complex issue, and government and private sector alone don't have all the answers. It will take everyone working together. However, we need to solicit input from many subject matter experts from outside of this team.

Mr. Roemer stated the Governor's focus continues to be ensuring this team has the most talented pipeline of cyber experts in the state and is doing everything we can to educate Arizonans. When it comes to cybersecurity, it is not a matter of if but when, so let's get to work.

3. MEMBER INTRODUCTIONS

Each member briefly introduced themselves and their positions.

4. TEAM MEETING MINUTES

Mr. Roemer stated that the team was unable to get last meeting's notes to the team members in a reasonable time before this meeting. The meeting minutes for the previous meeting will be reviewed at the next Arizona Cybersecurity Team meeting (12/20) along with a resubmittal of the summary of the three missions for each of the subgroups.

5. TEAM ACCOMPLISHMENTS

Mr.Romer briefly reviewed the accomplishments of the Arizona Cybersecurity Team thus far. The team has successfully identified three (3) subgroups, co-chairs, and charters, to enhance the team efforts further.

6. CYBER THREAT BRIEFING

Mr. Mike Lettman started the briefing by discussing the latest and most concerning attacks as related to cybersecurity threats since the last team meeting. Since the last meeting, many government entities have seen serious attacks including the Port of San Diego, and the State of Pennsylvania. Mr. Lettman also overviewed the importance of Cyber Liabilities Insurance for cities in light of these attacks.
Mr. Lettman addressed the breaches, standards, fines to cyber companies, and alerts that have happened recently. Breaches include the Apollo breach which exposed data of roughly 200million contacts, the City of St. Petersburg breach of residents' credit card information, and credit card breaches against CIOs and CISOs.

Mr. Lettman overviewed examples of cybersecurity standards that have either been implemented and can be an example or where standards may be helpful in the future. California has issued security rules around the Internet of things (IoT). Connecticut has done similar self-regulation around cybersecurity and internet connected devices. Mr. Lettman spoke about the need for across the board standards

such as NIST standards to address the ever-increasing reach of Internet devices and the integration of such devices in government, the private sector, and personal processes. One area the Federal government is actively looking to set NIST-like cybersecurity standards is in the area of Blockchain. Mr. Lettman reviewed fines being applied to cyber entities to increase cybersecurity and cyber accountability and touched on the FireEye reported APTs out of North Korea. The briefing addressed alerts specifically via the FBI IC3 advances in Precision Agricultural Increasing Vulnerabilities desktop protocol.

Mr. Lettman reviewed five (5) common questions that colleagues commonly ask cybersecurity professionals, and how cybersecurity professionals can answer.
Q1: Are we secure?
A1: Where you have been, what you have done & where you are going
Q2: How do we know if you have been breached?
A1: Who do we work with?
Q3: How do we compare to industry peers?
A3: Budgets & bottom lines - are we spending more or less?
Q4: Do we have enough resources for a cybersecurity program?
A4: Spending & risk protection intersection
Q5: How effective is our Security Program? Also, is it properly aligned?
A5: Use of NIST or comparable standards

Mr. Lettman broadly touched on how the State of Arizona approaches cybersecurity by building cyber visibility, filling security gaps, reducing overall cyber risks through an enterprise approach, and continually monitoring and measuring cyber strength.

Mr. Lettman showed the visual mapping of "RiskSense," used by the State of Arizona to monitor cyber risks at all 93 agencies, boards and commissions, and puts the cyber risk into a credit score which is easy to understand. We have made much effort in improving our score and decreasing our risk.

Mr. Lettman then addressed recent media attention on the mid-term elections and reports of cyber attacks. He highlighted that state governments do not run elections. The Secretary of State (SOS) is responsible for registering voters. The SOS validates candidates on the ballots. The election is then turned over to the counties, via the county recorders, who are responsible for tabulating votes. The SOS then validates the votes after the counties. The county and SOS work together to facilitate recounts when necessary, but the counties are the ones tabulating the votes again. Mr. Lettman commented that the most significant threat to our elections is the fear, unknown, and doubt (FUD) being sewn int the voting narrative through media headlines.

7. INTEL SHARING SUBGROUP CHAIR PRESENTATION AND DISCUSSION

Mr. Lettman stated subgroup presentations by restating that the prior direction from the committee was to have three (3) missions and then additional movements inside those missions and to bring the top ideas to the ACT meeting.

The Intel Sharing subgroup stated they have 18 confirmed members for participation in their subgroup. The presentation identified their primary areas of concentration as identifying cyber threats and recommending action items to citizens, governments, and businesses, opening communication lines for

cybersecurity awareness, and open communication of responses to cyber risks. Much of the team feedback centered around the need to create impactful messaging that will resonate with the public. The team brought up a need for citizen outreach and messaging campaigns. Mr. Roemer brought up the ability for team members and companies to get involved in spreading messaging through social media and communications efforts, to reach citizens of our state better. Many members of the team worked on how to figure out what messaging for cyber hygiene practices and awareness would look like, who would decide what messaging works, and how to spread that message.

Members of the team brought up concerns with ad hoc messaging campaigns without an agreed-upon direction and narrative. Mr. Roemer summarized the team's concerns and priorities as the volume of concerns, the necessity to break-through silos, selection of a path, and what resources are needed to get the subgroup and team to that place.? Mr. Hellmer noted that the FBI has channels that can be helpful once the subgroup works out the desired goal of the messaging.

8. NEW TECHNOLOGY SUBGROUP CHAIR PRESENTATION AND DISCUSSION

The New Technology subgroup stated they have 19 confirmed members for their subgroup. The presentation identified their primary areas of concentration as identifying cyber threats, issues of concern, and action items to improve experiences with Smart Cities, IoT, Autonomous products, Cloud Computing, Blockchain.

The subgroup plans to address threats and concerns associated with these different focus areas. Threats and concerns associated with these topics that include: 5G integration, Smart City systems, mesh networks used by IoT devices, privacy threats, serverless and container management platforms, deep learning, and continuing to implement innovative technologies state-wide effectively. The subgroup plans to take a closer look at these and other issues inside new technologies.

The New Technology subgroup will suggest legislative and regulatory recommendations, public-private partnership recommendations, and other various recommendations as part of a dynamic response to future development.

ACT co-chairs, Mr. Lettman and Mr. Grimmelmann, stated that anyone not in the New Technology subgroup that has suggestions or comments on subgroup topics is welcome to bring these to either of the co-chairs.

9. WORKFORCE DEVELOPMENT SUBGROUP CHAIR PRESENTATION AND DISCUSSION

The workforce development subgroup will be presenting at the next meeting. They were unable to attend the meeting due to the schedule change.

10. OPEN DISCUSSION OF ADDITIONAL ITEMS

Ms. Slankas notified the group of the upcoming National Homeland Security Conference in Phoenix June 17-20 at the Phoenix Convention Center. This conference is an opportunity for the team and the state to showcase our State, Agencies, and Educational successes in cyberspace.

Ms. Figueroa informed the team of the Cybersecurity and Infrastructure Security Agency creation.

Dr. Haass was unable to attend but had a written statement read on his behalf. Dr. Haass addressed the desire for the team to work towards a roadmap for workforce & talent development, educational funding in K-12, vocational programs, and community college programs in cyber-related industries, and highlighting Arizona as the leader in cyber education and cyber excellence.

11. ADMINISTRATIVE ITEMS

The Team discussed future Meeting Date (Dec 20 and March 21) and said the next meeting would be used to discuss General Data Regulation Protections (GDPR), the Workforce development subgroup, and efforts in public outreach and messaging.

Mr. Lettman and the team stated that subgroups should each have ten ideas ready for the next meeting in December.

12. CALL TO THE PUBLIC

One member of the public inquired about a roadmap for the subgroups to follow, and efforts from the team to improve attracting and creating talented persons to Arizona including workforce development and mid-level engineers.

13. ADJOURN

The meeting adjourned at 11:00 AM.