CITIZENS PROPERTY INSURANCE CORPORATION

Summary Minutes of the
Information Systems Advisory Committee Meeting
Wednesday, June 7, 2017

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened telephonically on Wednesday, June 7, 2017 at 11:00 a.m. (EDT).

Roll was called and the following members of the ISAC committee were present telephonically.

James Holton (Chairman)
Freddie Schinz (Board)
Brian Foley (Advisor) [1]
Kelly Booten (*staff)*

Call Meeting to Order

Wendy Perry took roll.

1. **Approval of Prior Meeting's Minutes**

Chairman Holton asked if there were any corrections or changes to the prior minutes. There being none, he asked for a motion to approve the minutes from the March 14, 2017 meeting.

Freddie Schinz made a motion to approve the March 14, 2017, Information Systems Advisory Committee (ISAC) Minutes. Brian Foley seconded the motion. The minutes were unanimously approved.

Chairman Holton turned the floor over to Kelly Booten for the IT Security Update.

2. **IT Security Update**

Kelly Booten: Good morning, Kelly Booten for the record. Before I provide an introduction to the IT security update I would like to provide a quick audit finding status.

As of May there were no open IT audit findings. The two open items since the last report were closed, and IT is assisting the business in closing an item assigned to the claims unit. Big progress there.

Today we would like to provide an update on our IT security program which has progressed significantly over the last few years. The program is multifaceted and risk based with focus on governance, compliance, industry standards, security controls and a heavy emphasis on

[1] Brian Foley was not present for roll call, but later joined the teleconference at 11:03 a.m.

awareness and education. And, in case an incident does happen, we have a tested and well thought out Enterprise Data Incident Response Plan in place.

Today, Robert will provide an overview of the program and wrap up with our posture regarding the recent global ransomware events.

Robert Sellers: Good afternoon, Governors, this is Robert Sellers, Vice-President of Information Technology. We are focused in the area of security today. The presentation that I would like to give you, and provide any discussion on, is the overall posture of Citizens with respect to security management.

On page 2, I want to lead off with the information about how we monitor and manage security programs here at Citizens. We focus on a number of different control areas. We have a continuous audit function running against information security and it takes place by four different focus areas.

The Auditor General, as you know, has a regularly scheduled audit program for Citizens. Inclusive in that is Information Security.

Through the Office of Insurance Regulation, part of the Florida Department of Financial Services, we have the market conduct audit, which also runs on a regularly scheduled program. Again, Information Security is a component of that audit.

Our financial statements, produced by Dickens, Hughes, Goodman every year, accomplishes a financial audit. Again, Information Security and appropriate controls over access to data is one of the components of their audit.

Internally, underneath Joe Martins, the Office of Internal Audit program continually runs different audits and advisories that are reviewed with the Board at the Audit Committee, as well as individually as is required. So there is a significant amount of oversight into the Information Security and Data Security and Privacy in the organization by third parties to ensure that we are accomplishing the missions of the program on an ongoing basis.

We also focus on continuous risk management. Looking at third parties, again, to help identify any vulnerabilities in our posture, experts that are doing this every day for multi-national, global companies will review our posture on the technical side, scans against our internet presence, and scans against our internal systems.

We have upcoming a penetration test that we are going out for quotes on right now for the third quarter 2017 program. We have penetration tests that are accomplished as part of that. In 2015, we completed one and again we will complete one this year. Again, focusing is on whether there are vulnerabilities that, as part of our due diligence and as part of our practice, we have not discovered that a third party might be able to discover and then give us referenceable activity to go in and do corrections on.

One of the things I want to make clear in both the audit activity and the risk management activity is when we identify a situation that presents a risk factor to Citizens, we measure and score that particular risk. Anything up in the high level or critical levels goes immediately into a correction and mitigation program that takes a priority activity over many of the other things that we do inside the technology organization. So these identified issues go through that correction process.

Now, how do we know how we are doing? One of the challenges, of course, is to look at ourselves as a unique organization, given our mission at Citizens in the insurance space. We are able to compare ourselves with other insurance organizations, with other financial organizations that are delivering similar and same type services with internet presence, with types of data that we are managing, the sensitive data, the privacy data, et cetera.

We use two different forms of benchmarking. Gartner Technologies – they are a predominant firm in research and analysis for IT organizations, looking at information security as a specific area. We will see, a little further on, how we do our benchmarking using the Gartner program. The FFIEC Cyber Security Benchmark, which is a financial institutions council, provides a benchmarking capability, as well. Each year we look at how we are doing compared to other organizations in our posture.

On slide 3 in the oversight and feedback loops, clearly we have heard from the Board over the last few years about the level of importance you place on cyber security and the level of importance that our executive leadership team here at Citizens places on cyber security and risk. We work that down through our third parties, the OIA external entities that I was just discussing previously, and down to our internal IT governance functions. All focusing on: are we doing the right things around cyber security; are we achieving the goals that are being set by the Board and other entities for security.

So this covers everything from the steering activities all the way down through the operational standards, and it is a feedback loop as we are reporting back to you today, other information will continue to flow down to our leadership team here.

Slide 4 is the Gartner IT Score. I want to spend a little bit of time on this particular spider graph. There are three components to this graph. As you look around the external edge of the graph you will see the different domains of information security, starting with security governance in the 12:00 o'clock position, working down through planning, architecture, event detection all the way back up to risk and controls assessment.

The colored lines indicate the scoring that has gone on for the different components across a period of time. The red indicates the insurance industry. Gartner has collected and done assessments against a number of insurance companies across the world, and has identified where they are in their maturity for these areas, these domains.

In 2016, we performed a scoring exercise here at Citizens using this benchmarking program, and identified where we were at that time. Underneath Curt Overpeck and Mitch Brockbank's

activity, Mitch Brockbank is the Director of Information Security and Risk, they established a strategic plan for information security identifying improvements in these areas.
Over the course of the last year, we have gone through a rescoring activity here in May, using individuals out of the information security organization and our internal audit organization to identify where we are positioned today and we can see measurable improvements in areas that were focused on in the area of security governance down through organization, the controls and the engineering areas which were the initial targets of the strategic plan.

As we work our way across and over to the left we see other areas. Event detection and threat vulnerability and risk controls where we are seeing improvements, but those are still activities that are targeted for further activity here in the third and fourth quarter of 2017 and early 2018. We are seeing improvements based upon the program. We are seeing Citizens as a whole sitting in a good posture. We will continue to improve these areas as we go forward, and then we will also continue with our benchmarking activities as well.

At this point I would open up to any questions that the Board might have.

Chairman Holton: Any questions for Robert?

Jim Henderson: None here, Jim Henderson.

Chairman Holton: Hi, Jim, how are you? Welcome. Jim, any comments you would like to make? I know you have been really up to date on IT stuff and Security.

Jim Henderson: It seems like there is certainly leadership there reaching out to the right people on the testing evaluation. Security is a constantly changing environment based upon the different types of threats and it seems like the leadership and consultants are addressing that. I'm very pleased to hear about the focus of the attention here, spending time and effort and resources to make sure that the data we are entrusted with does not get into the wrong hands, and others cannot harm the company. It's good to hear the attention given to the issue.

Chairman Holton: That's good, and thanks for those comments. Good work to you, Robert, and your team for an exceptional job.

One question I had is the potential vulnerability of agents within our system. I assume there is continuing dialogue with the agent community and associations regarding potential issues from their end like ransomware type things and not opening up strange e-mails, that type of program, correct?

Robert Sellers: That is correct. Carl Rockman, the head of our agency group, has continued to work with the different agency organizations around the state, specific agencies, themselves, helping to educate. We are providing information on an ongoing basis to him and his team that provides them with details that can be used in that education process. It is a multi-faceted program, as you indicated. We have not only our internal stakeholders here at Citizens, we have our external agencies and agents. We also have, of course, the policyholders that are dependent upon Citizens and the agents to protect and manage their data appropriately.

Chairman Holton: Okay, great. Any other questions or comments?

Robert Sellers: Yes, Governor Holton, I would like to continue starting on page 5, as well. I have got a few other things to discuss.

Chairman Holton: I understand, yes, I was just giving the opportunity on this briefing to just conclude if there were any further questions. Please continue.

Robert Sellers: Okay, thank you.

On slide 5, there is a quick benchmark on IT security staff. We are managing with an appropriately sized staff of 13 FTEs. Again, looking at the benchmarks we are within alignment to the benchmarks of other organizations of our size.

I would like to call out the highlighted box there. We have been very fortunate in being able to attract and retain individuals in our security program that have a significant history with information security. As you indicated, threats continually change. These are people that have had time in position to mature, to understand how that evolves over time and to help us with our posture as it continues to evolve.

Slide 6 shows some of the activities that we are continuing with in the current program. As I indicated at the beginning, we do have a security strategy which is a formal, three-year plan. It does have a number of assigned tasks and projects associated with it, and I would be happy to cover those individually, as necessary, with anyone that would like further detail on that.

Within the program there are annual activities that are indicated by bullets, everything from the risk assessments which are ongoing, internal assessments of applications and technology looking for risk areas to Security Awareness programs, which is a significant part of preparing an organization to prevent potential risks coming into the organization.

Every Monday morning as an example, an e-mail goes out from the security organization with a new “how to” or a new “advice” component on how to manage risks individually as they go about their daily work.

We are doing significant work in the area of our penetration and vulnerability scans. We meet monthly to review the status of those, looking at measures and key performance indicators, and we continually review what we are going to do next and what is appropriate for the program. One thing I would like to call out at the bottom of the slide is the AIM Project. One of the things the Committee has seen over the course of a number of business audit areas, as well as technology audit areas, has been in the area of credentialing.

Concerns were raised over who has access to information, when they should get that access and when that access should be removed, and doing that in a timely fashion. This project is aimed specifically at handling that and in putting the appropriate processes in place.

We have staffed that appropriately at this time and they are continuing to work through that to ensure we have improvements in the credentialing activity. That is really the first place you have to start - appropriate access to data.

Slide 7 is the Security Risk Assessment Activities. Again, we look at a number of different risks on an ongoing basis, and as I indicated at the beginning, we have third parties doing it for us and we have our own individual security teams doing it, as well.

We are looking at everything from the threats and the risks and the tolerance that the organization is willing to accept all the way down to how we are doing with the critical controls at the individual technology levels. So, it really is a program that covers the breadth of information technology and business technology to ensure that we have all aspects covered in looking at risks in all of those different areas.

Slide 8 - Successes in the program. Speaking specifically to governance, the Security Committee was put in place and is providing the guidance necessary to the program. We are benchmarking to ensure that we can measure how we are doing. The ongoing awareness that I mentioned earlier is continuing, and we run, not just the weekly blast, but we have programs around security awareness that are required training, certification type activity that has to be done at the beginning of each year.

The fourth bullet there, I think, is very important and I am going to speak to that at the end of the presentation, but within Citizens, knock on wood, overall Citizens has been very fortunate to have a very low activity around malware and ransomware impacts given the breadth of those across the world. We have been fortunate and I think it goes to our preparedness for that activity.

And then the last bullet - when something does occur we are prepared. We have cyber risk insurance in place. We have incident response plans in place that have been exercised, both in a formal exercise, as well as in an actual situation. So we have the necessary skills, people, processes and technology in place to handle an event if one were to occur.

Lastly, on slide 9, we look at continued success. How do we continue to make this program provide the capabilities that are needed by the organization? It first starts with these type of meetings here today, as well as your individual meetings with Kelly and Barry and others, with the Board awareness and support of these programs.

They do cost and have a financial impact on expense, but they are important to the organization. The executive engagement is also important. We brief the ELT members on an ongoing basis through our IT Steering Committee and Governance Committee as to where we are on risk and security. We have our plans in place and we are operating to those plans.

We have complimentary programs from our external providers in a number of different areas. As mentioned earlier, from agency management, as well as vendor management, internal audit and others that are important in carrying out this program.

Going to the last bullet on this slide - ensuring that our staff is engaged, that they understand the importance of information security, and the risks and responsibilities that they have with respect to our customers' data and their own personal data that resides in our systems. We believe that that is making a significant headway in the organization.

The newspaper reports do a lot to help us with that, as well. As you all are aware, even over the last couple of days, privacy and information security breaches have made the national news, once again.

What I would like to do at this point is cover, on slide 10, the recent events from 05/12 through 05/15, which, back in May, were the Twitter of information security dealing with the global ransomware event, and what Citizens' posture was at the time, how we responded to that and the impacts on that to us at this point. On Friday afternoon on 05/12, the newspapers and the internet media started to broadcast that there was a problem in the ransomware space - this is something that is ongoing all the time, but this was an elevated presence that had been observed starting the prior Wednesday and manifested itself in the alerts going out on the Friday, and it was impacting a number of organizations.

What was happening, at that point in time, was that computers were basically being locked out of access to their systems and data, and being presented with a message, pay me in order to return access to them. The impact to Citizens, at that point, was that we received notification through third parties, as well as our own internal teams, that the event was taking place.

We reviewed and did an assessment of our systems. Anytime we have an event of that magnitude we will reassess what our posture is and what our preventive measures are. In our case we have a number of different check points along the way taking place from the entry of e-mail into our system with preventative activity taking place there, all the way to scanning and virus activities that take place at the individual desktops.

We reviewed that to ensure they were functioning correctly, that they were catching the types of risks that were coming in, and felt that at that time that we had the preventative posture that was necessary to prevent that from taking place here at Citizens.

When we look at our preventative methods, the system patching activity is probably the number one preventative method for preventing a situation from occurring on an individual desktop or system. A large percentage of the world today uses Microsoft as their operating system and as their provider of services and solutions, and Microsoft has a regular patching program where they release security patches.

It is up to the individual organization like Citizens to take that information, to take those patches and to apply them regularly to the systems that they are running in their environment. We do that here at Citizens with our servers and our desktop platforms.

So, we felt that we were very comfortable with that particular attack profile. The end points had the appropriate malware and antivirus scanning and alerting processes in place. We had, as I mentioned, the internal e-mail protection systems in place. We had the security awareness

training, meaning that if somebody were to have had an event take place on their desktop, they knew the proper procedures to take to contact information security and the technology teams to prevent this from growing further into the organization.

Lastly, if we had had an event hit Citizens at that time, we have regular backup programs in place and our data secured in a way that we would be able to recover and that takes place on an ongoing basis. So, I am pleased to be able to say that for this particular event at this particular time we have not experienced any negative impact for Citizens.

This is just one example of a risk that is hitting us every day. We have many different organizations outside of Citizens who would like to be able to breach our security, to gain access to our data. This team's responsibility as they understand it, is to prevent that activity and to put in place the appropriate controls and measures to prevent that in the future, and to minimize any risk to the organization if something like that were to occur.

Governors that is my briefing for today. Kelly and I, Mitch and others are always available to you individually to brief you on any specific set of information that you would like. So thank you.

Chairman Holton: Thanks, Robert, for a very, very thorough and complete presentation. Good to have all of that knowledge, and thanks also to your guys for their very proactive efforts in guarding our systems against cyberattack.

Any questions for Robert before we move on?

Kelly Booten: Governor Holton.

Chairman Holton: Yes.

Kelly Booten: This is Kelly. I just want to add that we have a lot more detail in our plans, in the activities that are underway, and if any Governor would like an individual briefing, we can go into further detail. If anyone would like to do that, please contact me and we can set it up.

Chairman Holton: Okay. That sounds good. Thanks, Kelly. Anything else? We will now go to item three, and get a briefing from Sarah Harrell on Centerpoint.

3. **Centerpoint Update**

Sarah Harrell: Good morning, Sarah Harrell for the record, Director of Enterprise Programs.

Since our last Centerpoint update in March, we delivered Phase 1, which is the Financial Procurement phase. As you can see from slide two in the presentation, we completed our testing, our training delivery, and went live on April 3rd.

We celebrated, and our 90-day warranty support period from our vendor ended on Friday, and we have only three open items that they are currently working to resolve and then the phase will essentially be done and closed.

Great success for Citizens. There is a fabulous team behind me making this all happen. I can't give kudos enough to them, a fabulous team.

Phase four, which is Human Capital Management and Projects, has been kicked off. You can probably see that the milestone is a very similar process that we are going to follow for delivery of phase four. We had to kick off, we are in the discovery in process modeling stage right now and our target go live is 12/18. So we will go live before the end of the year.

And the magic about the date of 12/18, is that it is the beginning of the first pay period in 2019. So that is why we have to go live on 2018.

Kelly Booten: It is 2017 for 2018.

Sarah Harrell: Correct, thank you, Kelly. Slide three is Phase 2 Advanced Procurement also known as Vendor Management and Contracts. We kicked that off this week and are in the discovery phases for that. Our target go live for that phase is early November of 2017.

Phase 3 Budget will kick off in July. We did have a date change on that kick off. We slid everything out month because of some resource constraints on the vendor's side and it actually works better for us. So our target go-live date is now early February 2018, instead of January 2018. There are no costs associated with that date change, no business impact whatsoever. We just slid everything out a month.

Phase 5 is Advanced Human Capital Management, and we plan to kick that off in August. We haven't determined our go-live date for that yet. We are actually evaluating changing that go-live date for a number of reasons, and as that evolves I will keep you posted.

Slide four is the now infamous milestone slide that you have seen numerous times, and again, the salient observation is the work we have on our plate for the remainder of the year. We have four phases in flight at the same time for four months during the remainder of the year. Busy time, but we will make it happen.

Slide 5 is the approved action item with which you are also familiar.

Slide 6 is just an update on where we are on the payment of the costs related to the action item. Again, nothing magic about this. This is a fixed price, fixed bid contract so the payments are scheduled, the vendor is not going to miss them. We pay them when we are supposed to.

The notable point on this slide is our contingency spend. I have some comments there at the bottom of the slide. Contingency spend is just shy of $200,000 at this point and we have almost two million in the bucket. So well, well, well below what we would expect to consume from a contingency spend perspective.

The final slide is the projected spend for the remainder for the 10-year contract.

That concludes my update. Any questions from anyone?

Chairman Holton: Thanks, Sarah. Very good, the presentation and again, kudos to your team in getting this implemented very effectively. Any questions for Sarah? None being heard we are on to the final item which is New Business.

4. New Business

Chairman Holton: Are there any members who would like to raise anything before we adjourn? With none being heard, I will remind everyone that we will have a teleconference prior to the September 27th Board of Governor's meeting. I look forward to seeing everyone later this month at the June meeting. **If there is nothing else, I will entertain a motion to adjourn.**

Freddie Schinz made the motion to adjourn, Brian Foley seconded and Chairman Holton adjourned the meeting.

(Whereupon, the meeting was concluded.)