

CITIZENS PROPERTY INSURANCE CORPORATION

**Summary Minutes of the
Information Systems Advisory Committee Meeting
Tuesday, December 3, 2019**

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened telephonically on Tuesday, December 3, 2019 at 10:00 a.m. (ET).

The following members of the Information Systems Advisory Committee were present telephonically:

James Holton, Chair
John Wortman
William Kastroll¹
John Vaughan
Brian Foley
Kelly Booten, *staff*

The following Citizens staff members were present telephonically:

Aditya Gavvala
Carlos Rodriguez
Robert Sellers
Sarah Harrell
Stephen Guth
Wendy Perry

Call Meeting to Order

Roll was called. Chairman Jim Holton, Governor John Wortman, Governor Will Kastroll and Technical Advisors John Vaughan and Brian Foley, were present. Chairman Holton called the meeting to order.

1. Approval of Prior Meeting's Minutes

Chairman Holton: Welcome everyone to the December ISAC teleconference. The first order of business is approval of the prior Minutes. Any corrections? If not, I will entertain a motion.

John Wortman made a motion to approve the September 10, 2019, Information Systems Advisory Committee (ISAC) Minutes. John Vaughan seconded the motion. The minutes were unanimously approved.

Chairman Holton: The Chair will recognize Kelly Booten for the Chief Systems and Operations Update.

¹ Will Kastroll joined the call after roll was taken.

2. Chief Systems and Operations Update

Kelly Booten: Good morning, Kelly Booten, Chief Systems and Operations for the record. During the last quarter of the year we in IT and across the organization focused on planning, assessing and budgeting. Today I would like to highlight some of the activities in flight.

First is IT alignment to the Enterprise Strategic Plan and budgeting process. Jennifer Montero and I will be presenting the enterprise planning process and 2020 budget at the December Board meeting. IT's plan and budget are aligned to the enterprise plan with focus on the Key Strategic Initiatives for 2020.

We are currently in the process of revamping the IT Strategic Plan and intend to present it at a future ISAC. You have seen many of the components of the current plan through strategy presentations and overviews.

Some of the strategies we are currently focused on include:

- a. The cloud strategy, presented at the last meeting and planned for future meetings in 2020, includes a movement of our infrastructure to the cloud, but also must consider major application migrations such as Citizens' Insurance Suite. We recently attended the Guidewire Connection Conference and have started having strategy meetings with the vendor to understand their roadmap as we consider our options for migrating the suite to the cloud.
- b. The Identity and Access Management Strategy, which Robert and Carlos will be presenting today, is the outcome of our partnership with Gartner Consulting Services.
- c. In the works is the new Data & Analytics Strategy to employ predictive analytics that enable metrics driven front-end decision-making guidance in areas including fraud analytics and underwriting.
- d. In partnership with HR, IT is focused on two strategies to help ensure we have the necessary talent, skills and capabilities to balance the supply and demand of key talent over time. One is the GROW program to develop a talent pipeline in IT with local relationships such as FSCJ to fill niche positions that are hard to recruit or retain. IT will also be a pilot for a Strategic Workforce Planning initiative led by HR.

In addition, through our Gartner EXP membership, we are benchmarking IT costs utilizing what is known as IT Cost Optimization and the Gartner IT Score tool to compare Citizens' costs to other insurance companies. The main objective is to balance between reducing IT costs and investing in technology that will reduce business costs. Aditya and his team have identified some quick wins and have a roadmap for continuing this initiative.

Today, I will be presenting the Technology, Infrastructure, Software, and Professional and Staff Augmentation Services Action Item for approval. This action item is the technology spend necessary to achieve our business objectives for the 2020 budget year.

That concludes my update, Governors. If there are no questions, I can turn it over to Robert.

Chairman Holton: Thanks. Any questions for Kelly? Thank you, Kelly. The Chair now recognizes Robert Sellers to provide the IAM update.

3. Identity & Access Management Update

Robert Sellers: Good morning Governors and Advisers. My name is Robert Sellers and my role here at Citizens as Chief Technology Officer includes the responsibilities for the strategic and day-to-day activities of our IT Security and Risk organization. The IT Security and Risk team itself is led by Carlos Rodriguez who is here with us today, and he is the Director of this area.

Members, before we get into the Identity and Access Management program update, which Carlos will deliver, I would like to cover a few points around Citizens' information security and risk posture at this time.

I will preface the following overview with the offer for individual, detailed briefings on our specific security and risk activities with any of the technical advisers and Board members at your request.

Charles Dickens had a famous opening line in the novel, *A Tale of Two Cities*. He started with, "It was the best of times and it was the worst of times," and it continued in this vein of contradictions for the length of the paragraph. Much like his visions of London and Paris, the current state of cyber security in the world today gives us much to think on and to act upon.

As technology and business have become intertwined, the confidentiality, the integrity and availability of Citizens information resources have never been as critical for the performance of our organization, and we have never had as many technology solutions available to help ensure this. And yet, the bad actors of the world have never had as many tools and resources at their fingertips to attempt to compromise these critical attributes.

They are continually pressing organizations in numerous areas, but three key areas of focus are breaches of information that we maintain and control, breaches of information that others maintain on our behalf, and the denial of our organization's access to both types of information through ransomware and other inappropriate activities.

Almost daily the mainstream press and technology media are full of examples of these and they are happening at a significant expense to the impacted organizations. Major focus points for Citizens have been and continue to be the assurance that private and confidential data is encrypted and protected and that appropriate access is controlled.

This means that the access to systems that maintain and process our data have the appropriate external and internal controls in place to prevent any inappropriate access. This includes access and other types of controls for our networks, our servers, our applications and data, and the end-user computing devices such as desktops, laptops and mobile devices.

We recently moved certain systems to the Microsoft Office 365 cloud and are now starting to leverage components of Microsoft's vast embedded security capabilities to strengthen our posture in these areas. We are regularly contracting with third parties to evaluate our maturity and test our control in these areas and our traditional data center systems through penetration testing activities.

As we move Citizens' systems further into the cloud as part of our cloud direction, we are continuing to validate and test the security controls for environments both on premise and in the cloud. The third parties maintaining our information on our behalf are also held to similar standards through our contractual terms and these are validated by third-party testing organizations.

Citizens regularly receives reports on the state of their risks and security controls. We also regularly track internal and external risks that have been identified, evaluate them for significance and mitigate those risks on an ongoing basis.

With thousands of individuals accessing our systems, we also have a strong commitment to IT security and risk education. We have a constant messaging and testing with our staff and other parties on situations they may encounter during their everyday tasks, such as phishing e-mails, maintaining good controls of their access credentials and the use of capabilities with different software that will provide for a more secure environment.

Monitoring our systems for inappropriate access and other inappropriate activities is a 24 by seven activity. We recently partnered with a third-party organization to enable a systematic process of constant review of our different systems and have a playbook in place that is being used to act whenever an event is identified as "interesting".

So, as you heard, our security team along with our entire IT team and the rest of Citizens is executing regularly to reduce the opportunity for a situation to occur, and we are prepared to act if needed.

Despite our best efforts to prevent an event, one could come at any time. One example might be a ransomware event where, through phishing or other method, malware obtains access to our systems and begins to encrypt files either on end-user devices or on our servers or other file systems.

Rapid identification that such activity is taking place would take place through our internal and external monitoring tools, and our partners and Citizens staff would execute a specific ransomware playbook that was built to address this type of event. This playbook includes executive level crisis management activities, as well as involvement from our legal and privacy team, the IT team and others as needed, and it involves processes and different types of technology we utilize today to recover from the event. We run tests periodically with the different teams to ensure readiness to execute, when necessary.

Governors, I have intentionally not mentioned any specific technology we are utilizing today in the area of Citizens' IT security. We have technology in place for the tracking and management of risks and for the control points of areas that I pointed out earlier.

We are constantly evaluating our posture and technical capabilities to execute against the current threat environment. And Carlos and his team are involved with numerous federal, state, industry and other third-party security and vendor organizations to provide Citizens with as complete a picture as possible on the risk areas that may need additional process or technology added or modified.

Carlos is going to brief on the critical area of identity and access management next. But this concludes my remarks and I will take any questions now or we can defer to the end of Carlos' briefing. Governor Holton, how would you like to proceed?

Chairman Holton: Members, any questions for Robert? Okay, none being heard, we will recognize Carlos then.

Carlos Rodriguez: Good morning, Governors and Advisers. My name is Carlos Rodriguez and I am the Director of IT Security and Risk. This is an update briefing on our Identity and Access Management program.

I want to start by calling upon a quote from Bill Gates who allegedly stated that, and I am paraphrasing here, "Most people overestimate what they can do in one year and underestimate what they can do in 10 years." That is certainly the case with this program, a long-term endeavor with focus on making a steady progress in continuing to mature our current state of identity and access over the next several years, while better positioning us to adjust to the current pace of technology change.

Starting on page 2, we will touch on the business objective driving IAM. As you may recall from Robert Sellers' update last quarter, our journey began in May and is a multi-year program with a phased approach. As you know, we engaged Gartner to assist us in reviewing our existing IAM strategy, to identify gaps, and provide us with a road map which we will explore later today.

We believe that this is a program that enables business capabilities. We don't necessarily see this program as a security project as shown in our business objectives. We believe that by improving the existing Citizens' identity and access management capabilities, as listed in each of the objectives, we will reduce overall risks to the organization in the cyber security and compliance areas while enhancing our capabilities to provide a better experience to our stakeholders.

So, we can now move to page 3 and take a look at the IAM overview. Our main goal with IAM, or identity and access, is simply to provide the right people with the right access at the right time while building automation to perform this where possible. The results of the Gartner gap analysis were recommendations in three key areas: authentication, administration management and access management.

Our approach to the delivery of this program includes performing retrospectives throughout the project and reforecasting on a yearly basis. Kelly Booten is the program sponsor, Robert Sellers is the owner and Sarah Harrell, from our Program Management office, will provide program management for the team. As part of the program we will be providing regular updates to the IT Steering Committee and the ISAC.

We can now move to the next page and take a look at the project implementation roadmap. So, now we can see the journey at a high level, and this is our projection as we mentioned.

First, we have three different swim lanes, and I want to remind you of that. They are Access Management, which is the oversight of who can access what resource based on their role and need to know basis; Administration Management, which is the management of user ID's and roles; and lastly, Authentication which is validating that you are who you claim to be.

So, starting at the top of this slide we see access management. Our target here is a replacement for the existing access system with a modern access management solution that is built for today's and future access needs and is cloud ready. We are going to target this for research in 2020 and implementation starting in 2021. Another aspect of access management is Privilege Access Management, which is around

improving our existing management of user accounts that have high privilege or access rights. We are already in the process of evaluating cloud ready solutions that we can migrate to next year.

At the middle of this screen in teal color we have Administration Management. This is where the processes, procedures and automation happen. This is also where we will bring all existing user access management together to a central team with robust automation tools for boarding, deboarding and compliance attestations. This will ensure that we will continually know who and why anyone has access and why they have the access. This will make everyone's role in access management more efficient and in addition to other benefits, will continue to ensure that we can quickly board our independent adjusters in a timely manner during a CAT event.

As for Authentication in the navy-blue section, we are already active in the early stages of delivering Multifactor Authentication or MFA to the organization for Microsoft 365 and Azure. Our target is to complete the implementation by the end of the first quarter of 2020.

Next, and frankly perhaps the most critical item in the slide is around the yellow diamonds you see on the slide. These are points where we know we will have to make critical technology decisions that will involve our IT Steering Committee and ISAC.

Finally, as Robert mentioned earlier, we are in the process of adopting Microsoft technologies that we acquired through our existing enterprise agreement. Their security solutions are an area that we will continue to evaluate through this program. For example, we are adopting the Microsoft tool for Multifactor Authentication and we will continue to evaluate others as the program matures.

We will now move to page 5 where we can look at the Value Attainment and Economic Considerations. In terms of the program financial impact, we expect to see positive impact in terms of:

- Reduction in overall risks as related to access and authorization
- Reduction in re-work and mitigations related to audit findings
- Decrease in time required by business staff to track and manage identity and access information
- Potential costs related to data breach response

Finally, we will be performing a financial analysis as part of each major sub-project as listed in the road map.

Governors, this concludes my presentation today. Are there any additional questions or comments?

Robert Sellers: Governor Holton, this is Robert Sellers. I just wanted to make a quick comment on item number four in this last list which is the potential costs related to data breach response.

Chairman Holton: Okay.

Robert Sellers: This is an area of research that we have been dealing with Gartner on as part of the service that they provide to us, and the dollar cost is staggering when you get into a data breach situation.

Their average that they have identified is \$225 per breached record. So, an organization with a million records potentially would have a staggering amount of impacted costs by the time they did all the mitigation and cleanup activity associated with that. So, without a doubt, one of our first goal objectives is to avoid that at all costs. I just wanted to bring that into light when we start talking about the scope and risks associated with inappropriate access.

Chairman Holton: Yes, that is an amazing number; an amazing, staggering, daunting number and obviously your analysis is going to include not only avoidance, but mitigation if a risk occurs of further problems, correct?

Robert Sellers: Correct.

Chairman Holton: Okay, great, thank you guys. Any other questions for Robert or Carlos?

Brian Foley: This is Brian Foley.

Chairman Holton: Go ahead, Brian.

Brian Foley: Robert, what frameworks are you using to guide what you think is needed? So, as a for instance, are you using ISO as the framework to figure out what components need to be in place, what controls, et cetera? I am assuming that there are, as there are in health care, there are guidelines produced by the government around property and casualty for specific compliance activities related to identity and access management that need to be governed, controlled, mitigated, et cetera. So, any comments you have on that?

Robert Sellers: Governors, Brian, we have a number of different frameworks that we utilize. I think one of the misconceptions out there is that any one framework itself will satisfy all the needs of the organization.

We have looked at this over many years looking at the different control frameworks and the specific security frameworks, from ISO, from NIST. We utilize the critical security control processes and methodologies that are available to us. We have gone through and identified what we believe to be of concern and highest risk to Citizens and have implemented controls in and around those areas.

These are also backed up by the review activities that both our internal auditors, under Joe Martins, execute against, as well as our external auditors from the State of Florida, the Auditor General and the Office of Insurance Regulation, and of course our regular financial audits.

So, when you ask which control, I would say many; which frameworks, I would say many. Components of each of those have been evaluated for its appropriateness to Citizens, and that includes in the financial world, as well. We are a member of both the MS-ISAC, which is the federal side, and we are also a member of the FS-ISAC, which is financial services. We use the controls and frameworks that are available from those, as well. Carlos, is there anything that you would like to add?

Carlos Rodriguez: Only that we are at the point in the cycle where we are evaluating our frameworks along with our legal department and our OIA. So, it is a partnership to continue to monitor the program.

Brian Foley: Very good. That is the answer that I expected. So, thank you.

Chairman Holton: Thank you. Any other questions? None being heard we will move on. Thanks again, guys, for a very thorough report. Next item is 4A and the Chair recognizes Aditya Gavvala to introduce the action items.

4. Action Item

a. Amendment to Existing Agreement for Software Maintenance and Support for Customized Insurance Management Licenses (Contract No. 19-18-2002-00) and Successor Agreement for Software Maintenance and Support for Customized Insurance Management Licenses

Aditya Gavvala: Good morning, Governors, I would like to draw your attention to tab four where we have the action items.

The first one is an amendment and a successor agreement. We have a legacy document repository process that houses over 300 million historical insurance documents. In order to provide this software, we will need to convert over 30 million documents stored in the vendors proprietary format to the standard PDF format. This requires a one-time professional services engagement with the vendor. We are requesting a \$66,000 amendment to the current contract; \$53,000 of that is towards data retrieval services, and we also have reserved \$13,000 as contingency fund.

In addition, we are also requesting to have a successor contract to extend the licenses of the software through the end of March in 2021. The requested funds are included in the proposed 2020 annual budget.

If there are no other questions, may I go for the recommendation?

Chairman Holton: One quick question I had, and I discussed this a little bit with Kelly in a pre-briefing. The total amount, especially for the data retrieval, Kelly and you guys had mentioned that's possibly the major ceiling for that, that it's possible to negotiate a little further in terms of the actual hard hour cost of the data retrieval once we get into this, so it could go down a little bit. Is that my understanding still?

Aditya Gavvala: It's an accurate statement. We know that we have over 30 million documents that need to be converted. So, when we presented our statistics to the vendor, the vendor then estimated their software dollars against that and came back with approximately \$53,000.

We have been working on opportunities to negotiate to bring that number down. The vendor realizes that this is the last straw, because once the software is retired, they will not have revenue from us. So, we are working with the vendor, our VMO office is diligently working with them to see if we could negotiate the numbers down.

Kelly Booten: And Governor Holton, if I might add. We also need to point out on the second page that this is a sole source contract and we publicly posted it. It doesn't become a final award until December 5th due to the time frame for protests. So, this --

Chairman Holton: Right.

Kelly Booten: -- action item needs to be contingent upon that going through and then, by the time of the Board meeting, that would have been resolved.

Chairman Holton: Gotcha, appreciate those clarifications. Any other questions prior to reading the action item? Okay, proceed with the recommendation.

Aditya Gavvala: Thank you. The staff requests that Citizens Information Systems Advisory Committee approve and recommends the Board approve the requested amendment to contract number 19-18-2002-00 for the total amount not to exceed \$66,000; approve a new successor contract with Vertafore for a one-year term of April 1st, 2020 through March 31st, 2021, for a total amount not to exceed \$51,000; and authorize staff to take any appropriate or necessary actions consistent with this action item.

Chairman Holton: Thank you. Having heard the action item, do I have a motion to approve?

John Wortman made a motion to approve the Amendment to Existing Agreement for Software Maintenance and Support for Customized Insurance Management Licenses (Contract No. 19-18-2002-00) and Successor Agreement for Software Maintenance and Support for Customized Insurance Management Licenses Action Item and Brian Foley seconded the motion. All were in favor. Motion carried.

Chairman Holton: Aditya you are still recognized to deliver agenda item 4B.

b. Oracle Fusion Managed Services

Aditya Gavvala: Yes, thank you. The next action item that I want to present is Oracle Fusion Managed Services contract amendment. Citizens today uses Oracle Fusion Enterprise Resource Diamond software to support human resources, financial accounting, budgeting, vendor management office and other IT areas.

In March of 2019, through an RFQ process, Citizens selected two vendors to provide ongoing application support services for our ERP system. After a one-month trial period, GCOM Software was determined by Citizens to provide the best value. This action item is seeking approval of the contract amendment to use GCOM Software for ongoing application maintenance, enhancements and support. The estimated contract amendment amount is \$2 million for a base term of five years. The action item is not seeking approval for the renewal term. A separate action item will be requested for any renewal and associated spend in the future. I will take any questions at this time.

Chairman Holton: Any questions on this item? Let's go ahead with the recommendation then, please.

Aditya Gavvala: Staff requests Citizens Information Systems Advisory Committee approve and recommends the Board approve the contract amendment for Phase II services to be provided by GCOM Software through an amendment to the contract number 19-19-5004-01 for a total cost not to exceed \$2 million dollars for the five-year base term ending September 18th, 2024; and authorize staff to take any appropriate or necessary actions consistent with this action item.

Chairman Holton: Thank you. Members, having heard the recommendation, is there a motion for approval?

John Wortman made a motion to approve the Oracle Fusion Managed Services Action Item and Brian Foley seconded the motion. All were in favor. Motion carried.

c. Technology, Infrastructure, Software, and Professional and Staff Augmentation Services

Chairman Holton: Thank you, Aditya. We now turn to the final action item and the Chair recognizes Kelly Booten to present this.

Kelly Booten: Good morning. This is the yearly action item that corresponds to the annual budget for items that will be purchased off of state term contract and alternative contract sources approved by the State of Florida Department of Management Services.

It also includes some services that will be purchased off existing Citizens-procured contracts. This is in the contract ID section of the action item. This year we brought forward all as an action item. In previous years we have had consent items plus a few action items, depending upon whether the contracts are new or renewing, and this year it was a combination of both, so we just included them all in one action item.

The funding for the requested Technology, Infrastructure, Software, and Professional and Staff Augmentation Services is requested in the amount of \$14,833,702 in the 2020 budget, and overall for the three-year term, \$18,022,337.

John Wortman: Kelly, isn't that think mean or 18 million?

Chairman Holton: 18 million.

Kelly Booten: Million, yes, sorry, million. \$18,022.337.

Kelly Booten: As further described in the contract amount section, we have broken it down by spend category - by infrastructure, software and professional and staff augmentation services. In each of those sections there is a paragraph that describes the major expenditures under each category. If you'd like, I could go into detail on any one of those items. We also have a spreadsheet of 198-line items that backup all of these expenditures that are included in our IT budget.

So, unless there are any questions, I will move on to the recommendation.

Chairman Holton: Members, any questions for Kelly prior to the recommendation? Okay, go ahead.

Kelly Booten: Staff requests that Citizens Information Systems Advisory Committee approve and recommends the Board approve the action item totaling \$18,022,337 and authorize staff to take any appropriate or necessary action consistent with this action item.

Chairman Holton: Thank you, Kelly. Members having heard the recommendation do I have a motion to approve?

John Wortman: This is John Wortman again. I just had one question, Kelly. You said this is kind of a combination of historical things. Is this price about the same as history?

Kelly Booten: Okay, so this one is interesting because there are some contracts on it that are multi-year and every year there are things renewing. So, there is a little bit of level setting you can do, but overall, yes, and even a little lower than historical.

Last year the total was \$29,771,560, and the 2019 budgeted amount was \$16,502,908. So, this is definitely less than last year, and we really worked hard, especially in the software area, of paring this down. However, last year had Microsoft on it so it had one, big, large expenditure that this year does not have, but overall, this is definitely reduced from last year.

John Wortman: So, this is probably close to five to seven million less than last year?

Kelly Booten: Correct. And if you look at further breaking it out a little bit, most of it is continuing operations, at least 12 million of it is continuing operations that are just part of what we do in IT.

John Wortman made a motion to approve the 2020 Technology, Infrastructure, Software, and Professional and Staff Augmentation Services Action Item and John Vaughan seconded the motion. All were in favor. Motion carried.

5. New Business

Chairman Holton: Our final agenda item is new business. Is there any new business to come before the good of the order? Okay, none being heard, I will remind everyone our next teleconference is scheduled for March 10 at 10:00 a.m. I hope everyone had a great Thanksgiving and look forward to seeing you at the Board meeting. Is there a motion to adjourn?

John Wortman made the motion to adjourn. Meeting adjourned.