**CITIZENS PROPERTY INSURANCE CORPORATION**

**Summary Minutes of the**
**Information Systems Advisory Committee Meeting**
**Tuesday, September 12, 2023**

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened via Zoom webinar on Tuesday, September 12, 2023, at 10:00 a.m. (ET).

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

Jason Butts, Chair
Nelson Telemaco
John Vaughan
Kelly Booten, staff

**The following Citizens staff members were present:**

Aditya Gavvala
Barbara Walker
Bonnie Gilliland
Eric Addison
Greg Rowe
Jay Adams
Jennifer Montero
Jeremy Pope
Joe Martins
Ken Tinkham
Ray Norris
Robert Sellers
Sarai Roszelle
Stephen Guth
Sudheer Kondabrolu
Tim Cerio
Violet Bloom
Wendy Perry

Roll was called and a quorum was present.

## 1. Approval of Prior Meeting's Minutes

**Chairman Butts:** Good morning, everyone. Thank you so much for attending the ISAC committee. To start, I would like to have an approval or a recommendation to approve the prior month's meeting Minutes, please.

**Governor Nelson Telemaco made a motion to approve the June 27, 2023, Information Systems Advisory Committee (ISAC) Minutes. John Vaughan seconded the motion. All were in favor, and the minutes were unanimously approved.**

**Chairman Butts**: With that we will turn it over to Kelly Booten.

## 2. Chief Operating Officer Update

**Kelly Booten**: Good morning, Kelly Booten for the record. Today I would like to provide a brief update on three technology initiatives that the Board recently authorized.

At the July 28th Board meeting, the Board approved Citizens Business Insurance Suite program. We will migrate our current on-premises Guidewire suite to the Guidewire hosting platform. This platform is used to provide the essential technologies and services that support Citizens'

underwriting, claims, billing, and policyholder functions: PolicyCenter®, ClaimCenter®, BillingCenter®, and the customer and agent portals.

All contracts have been executed by Citizens. The Master Agreement and Subscription Order have been signed by Guidewire. The Professional Services Agreement and Statement of Work are with Guidewire and are anticipated to be signed, hopefully, today but at a minimum, this week. Assuming contracts signature this week, kick off will then commence as early as next week with discovery running through the end of the year, then the technical upgrade is anticipated to start in January. We will continue to provide quarterly updates through the ISAC as this implementation progresses.

Also, at the July 28th Board meeting, the Board approved Citizens to contract with Applied Systems, Inc. for an intuitive next generation Citizens Eligibility Reimagine platform. The platform will support Citizens' obligation for a Clearinghouse program as required under Florida Statute. The platform will connect private market carriers to obtain quotes for new and renewal , and to determine if private market offers impact eligibility for Citizens.

Contracting is in progress whereby details of the phased implementation plans are being ironed out. We will provide an update at the Exposure Reduction Committee on September 26th with more specifics, and also an update on the interim Clearinghouse program recently implemented as a bridge between the old and new Clearinghouse platforms.

The third initiative, Unified Communications as a Service and Contact Center as a Service, also known as UCaaS and CCaaS, was approved by the ISAC and Board in November and December, respectively of 2022. UCaaS, a cloud-based platform by Verizon that unifies multiple communication channels including voice, video, and messaging, went live on August 7th. This platform replaces our ageing on-premises telephony system, reducing the risk associated with it, while also delivering superior capability and integration with our Microsoft platform.

The second phase of the project, virtual contact center or CCaaS, the call center operation in the cloud, recently kicked off. Discovery is in flight and implementation will most likely occur in first quarter of 2024.

In closing, today Robert will provide the annual update of our IT Security, Risk and Resiliency programs, and then Aditya will ask for approval of the annual Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part 1 action item.

That concludes my report.

**Chairman Butts:** Thanks, Kelly. Is it to Robert or to Aditya?

**Kelly Booten:** To Robert.

**Chairman Butts:** Great, Robert, to you, sir.

### 3. IT Security, Risk & Resiliency Update

**Robert Sellers:** Thank you and good morning. Today, I'm going to brief you on the IT Security, Risk, and Resiliency programs. Wendy Emanuelson, our Director of IT Security & Risk, is not with us today, unfortunately. The briefing I'll perform in its entirety.

The first thing I do want to mention to the Governors, as well as the Advisors, is that we are dealing with a sensitive topic here today. One, our information security posture and approach. I am available, as is Wendy and other members of our organization, to meet with you individually to discuss our detailed approaches to information security and risk and to cover any other ground that you would like to do so later.

Today's briefing will be a very high-level briefing, and we will encompass all three of these topics, IT security, risk, and enterprise resiliency.

I do want to also start with a comment that information security and risk here at Citizens is an enterprise-wide discipline. We work and partner with our Enterprise Risk Management organization under Joe Martins. We work with our partners in IT with Aditya's team across the organization for the implementation of the necessary tools and software for IT security and risk management. We also work with our legal organization to ensure that we're following appropriate statute and rules with respect to our compliance and other responsibilities that we have in our area of operations.

Then finally, we also work with many of the different control organizations that review our information security including the Auditor General of the State of Florida, as well as the Office of Insurance Regulation in their market conduct studies. They identify and review our IT posture, and of course, we have our own internal audit organization that performs IT controls review on a regular basis looking to ensure compliance to our policies and regulations and standards. Let's go ahead to the next slide, please.

What we do - this is a substantial look at activities and responsibilities that we have inside information security that covers our operational area and our enterprise resiliency, which is focused on several topics. I will go into more detail here, as well as our governance risk and compliance areas. We're formed with great teams in the IT Security & Risk organization that are focused on each one of these areas. You'll hear a little bit later about some of our activities around building capabilities within our organization to allow IT team members to perform more risk management activities. These areas are covered by two major architecture areas, and at the last ISAC meeting you met Chris Jobczynski who is our Director of Enterprise Architecture & IT Strategy. The architects within our application security and solutions areas work in tandem with our enterprise architecture group to ensure that we have alignment across the organization with a high-level perspective as we're moving through building systems applications in support of our policyholders and our other stakeholders. Let's go ahead to the next slide, please.

The IT Security & Risk Strategy is a bit of a moving target. IT security is being challenged like never before from the different threat actors. Some of you may have seen this morning the MGM Grand attack that has impacted their entire operation. This is a major international organization that is dependent upon customer service and website capabilities to manage their organization, provide services to their guests, and manage their gaming solutions. There are constant threats, and we do everything in our power through our tools, our training, our exercises to prevent an occurrence. Our strategy is constantly evolving because the threat actors and actions themselves are constantly changing. With the recent advances in artificial intelligence, the threat actors are now using those tools to enhance their capabilities, and we are having to respond and react and continually work to stay ahead of them. The number of attacks that we prevent daily between the external networks and phishing attacks or e-mail are astounding.

As we work through these attacks, our goal is to protect our data which is ultimately our policyholders' information. We ensure confidentiality, we ensure the integrity of the data in our operations, and we ensure the availability of that information, and so the strategy here continues to be focused on those items.

As we move down to the “What?” in the middle of the slide, you will see three objectives. You will also see those a little bit further down in the presentation where I will focus more on what we are doing, where we will be focused in the next year on advances to continually stay ahead of those threat actors, and how we will continue to improve our capabilities.

We have an execution approach, and you can see where the process is the standard “Identify, Protect, Detect, Respond, and Recover” process and then we start the cycle all over again. We have principles associated with our IT security risks and we also have principles around our resiliency plan. We can protect but at some point, we do have threat actors who, through a phishing campaign, for example, are able to acquire and access a machine. We identify, we shut that down, but we must plan for how to deal with that type of attack and that’s our reason for this type of process. This is one small example. A larger example is our approach to resiliency execution, which is something of significant size to the organization. One example of that type is our recent claims IT CAT response. Let’s go ahead to the next slide unless there are any questions at this point.

Objective 1 is continuing to build strength in our teams. How are we doing that? Over the process with different organizations, we have different work groups and different types of training opportunities. We go through the knowledge sharing meetings bi-weekly with different teams.

We go through and perform educational activities, utilizing automation where possible. We train across both teams and individuals. In a security incident, teams react faster than individuals and where appropriate threat machinery or automation are in place, those type of tools can react faster and immediately respond on identification of a threat.

We’re building team resiliency through cross training. I mentioned this earlier, and it is an important part of our organization’s readiness. With the number of people that we have in the IT organization, as well as across the organization, there are hundreds of different people accessing our systems and working with our data. It is important that the organization itself understands what signals they’re looking for, what we’re seeing, what type of threats are out there and how they as individuals and teams are part of the solution to identify and respond. So, we take that all the way down to each individual employee and their specific responsibilities for security and risk.

And then the last piece is the “value” component as part of our collaborative environment. We’re focused on how collaborative based value of IT Security is improving risk management for our organization as we move from the reactive approach to a proactive approach. We use different types of research and advisory services from organizations such as the FS-ISAC, an organization established for Financial Service IT Security organizations to help establish where value can be obtained. So, this is a major objective over the course of the next year to two years for the IT Security strategy. Let's go ahead to the next slide, please.

Objective 2 is our security operations optimization. This past year we had a third-party vendor come in and do an assessment of our IT security operations organization and processes. They were very complimentary in terms of what we had in place already.

Looking down at the left side of this slide you can see the current state. It is a robust architecture, we have highly skilled analysts, and we have several maturity assessments that were already completed to help self-identify opportunities for improvements. The other thing that is very important in security operations optimization is executive support. We have that throughout the organization from Kelly, of course, with her responsibilities as Chief Operating Officer with IT, but also by Tim and our Chief Counsel, and by Joe Martins and other leaders in the organization.

Over on the right side, the in-progress activities, we are working on optimizing our tool set. We're focusing on a single pane of glass approach. For any individual that has experience with operating machinery or operating equipment, trying to obtain intelligence about what is going on and respond at the same time, you recognize that having that single pane of glass for the operator will be a significant time saver and will improve efficiency in response. This reflects the reduced vulnerability time that we have in the organization or rather, our time to react and respond to an event. Security Operations is constantly seeing different types of threats - how do we identify what is an important vulnerability that we need to correct, what is an important threat or a high priority threat that we need to take further action on. Making that visible to the stakeholders and understanding the cost and timeframe that it takes to do those type activities is part of the improved metric area we are establishing.

And in the improved area of vulnerability management, I think as long as people have been writing software or creating hardware, vulnerabilities have been created. Part of this is understanding what the vulnerabilities are for the software that we utilize in this organization, ensuring that we are managing that appropriately, and resolving those vulnerabilities on a timely basis. In this world today, it's not just our software that we're running that's of critical importance to us, it's also our third-party vendors' software and processes that are out there. We've had a print vendor who had a significant event. It had an impact on Citizens. We've had other vendors that have had significant events that have had downstream impacts on our operations. So, not only are we monitoring and managing from a security operations approach within our own internal operations, but we must have the visibility and management of our third parties out there that are supporting us.

So, our security operations is a fundamental activity for the next several years to improve our capabilities in this area. Let's go ahead to objective three, please. Next slide.

In this objective we are working on continuing to improve our organization through resiliency and ability to respond. We have a number of different threats that can impact us at any time, whether it's an accident on a bridge in Jacksonville that would prevent our staff from getting to our buildings for their daily operations, to a hurricane like we just had here in north Florida. We must develop resilient resiliency plans to address those to be prepared to respond, and then to be prepared to recover the organization back to normal state. We test and we exercise these activities on a regular basis. We just completed a failover of our insurance suite. As you can imagine, we do 99.999 percent of our business using our Citizens Insurance Suite today. If we were to have difficulties with that system, our ability to move to an alternative site and continue processing would be important, so we continually test those areas of software and systems and processes that might challenge Citizens. We have, as well, recently responded to the hurricane here in north Florida. Last year we responded to the hurricane in south Florida and performed numerous IT CAT response activities with Jay and his Claims organization and other parts of the organization.

So, the program updates we are continually preparing. That is really the main thing I want to leave you with, that we identify, we ensure the resiliency strategies are in place, we test them and then we are prepared to react to the different threats. Every year we do a gap analysis, and we go through an improvement cycle and a readiness cycle. This year we had over 160 items on our

readiness check list for CAT response from an IT system and process perspective that were completed prior to the first storm this year. Let's go ahead and continue to the next slide.

One area focused on our readiness testing given the Citizens growth. It was identified in our scenario planning activities the need to be continually ready for growth in policies as well as our ability to support a major CAT event. We would need to be able to provide capabilities for over 1.5 million active policies as well as a 425,000-claim event which would be very, very significant in size for our organization. Our teams evaluated and tested the systems to validate that capability, and we did that prior to storm season this year. Let's go ahead to the next slide.

These are the activities that we have going on over the course of the next several years. We have a flagship project which y'all have been briefed on previously, which is our Identity and Access Management Program. That program is being led through our Services and Delivery organization under Aditya focused on replacing our access authorization and management of credentials for all of our different systems across the organization. We have other activities identified for our application security programs, ensuring that applications that are being developed are being developed with security standards, as well as other activities around our governance and risk management which are focused on compliance. That answers the question, are we doing the things that we said we would be doing and the standards so that we are in fact compliant with those?

The last thing that I would like to mention is end user computing which is up in the upper right underneath the Governance, Risk & Compliance area. End User Computing with the advent of tools within software like Microsoft and some of the tools are available there and enabling this type of computing. There are also other applications that we use inside Citizens that are allowing our end user community to do more sophisticated development with the support of IT and those efforts bring different types of risks. Part of the education that we have with our staff is the responsibilities that they have for the security and risk management of any systems or any tools that they develop themselves. We are seeing more of this in our environment and part of our responsibility is to ensure that we're ready for that and that we are doing the necessary things for the organization to protect itself.

With that, Chairman, that completes my report. If there are any questions, I would be happy to take those today, or as I mentioned at the beginning, to meet with y'all individually.

**Chairman Butts:** All right. Thank you, Robert. Any questions for Robert? No, seeing none, we will move over to Aditya.

## 4. Action Item

### a. Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part I [AI]

**Aditya Gavvala:** Hello, good morning. This is Aditya Gavala, CIO for the record. Today I would like to present the Technology Infrastructure, Software, and Professional and Staff Augmentation Services - Part I Omnibus Action Item to the committee. Let's go to the next slide, please.

Let me begin with some background first. Since 2009, Citizens has requested Board approval for technology goods and services via an Omnibus approach combining the approval of technology related spend items through a single action item or consent item at the December board meeting. Based on a board member's request back in March of 2020 at a BOG meeting for additional time

for item approvals, Citizens began taking a two-part approach to align with the board member's request. Next slide, please.

There are two parts to our action item. The first part is primarily focused on anticipated purchases from January to April of 2024. The second part will be focused on anticipated purchases from May through December 2024. Please note that Part II is an estimate only based on the information that is available at this time. It is included in the presentation for the sake of completeness. Part I is what we are seeking the approval on at this meeting today. Part II will come to the December board for approval with final numbers. The projected spend in both parts is categorized into three parts: Infrastructure, Software, Professional Services and Staff Augmentation. Next slide, please.

On the top left corner, you see the total projected spend authority needed for the year 2024 as $31.5 million dollars. Part I is $24.5 million and Part II is $7 million dollars - that is estimated. The makeup of the total spend authority is shown at the bottom left corner. The three categories of spend are Infrastructure $7.7 million dollars, Software $15.9 million dollars, and Professional Services and Staff Augmentation combined is $7.9 million dollars. The makeup of Part I and the estimated Part II are shown on the right-hand side, and they are also on the next slide, so let's go to the next slide, please.

On this slide we provide low level details behind three major components of each of these spend categories. Major elements of the infrastructure components are refreshing the end-of-life components, data/internet services, and data center services. Major elements of the software are server and desktop platforms, virtualization software, Microsoft subscription, software as a service, technologies that we use, risk and security software, application software, middleware, and productivity tools. Professional Services and Staff Augmentation Services are used to support major Citizens' initiatives such as Enterprise Litigation Management, Fraud Analytics, Citizens Eligibility Reimagined, Identity and Access Management, and also further technology support. Next slide, please.

I would like to describe the resource strategy that is used at Citizens. You see at the bottom of that pyramid, Citizens' staff (full time employees) drive the delivery of all our major initiatives while balancing resource composition based on criticality of the initiative, time-to-market requirements, skill sets, and the support needs. We also use staff augmentation services to accelerate delivery of the major flagships business initiatives. Professional services are used for ongoing system maintenance and enhancements. Next slide, please.

Here we show the comparison of the total spend authority, this combines both Part I and Part II, 2023 versus 2024. There is a delta of $480,000 between 2023 and 2024. Part II numbers are shown on this slide but like I said, they are estimated numbers only and the final numbers will be presented in December.

The next slide explains the differences between the 2023 and 2024 action items. On the left-hand side you can see that Part I totals are higher; however, Part II totals are anticipated to be lower. The explanation is on the right-hand side. There is an increase in software due to multi-year renewals and a couple of new tools planned for procurement in 2024; however, there is a reduction in infrastructure, professional services, and staff augmentation. The Delta in the combined totals between 2023 and 2024 is $480,000.

That is the end of my slide deck. I will take any questions at this time before proceeding to read the recommendation.

**John Vaughan:** Yes, this is John Vaughan. I've got one question, and it's probably a little bit of a complex question. I could sit there, and I could bridge between 2023 and 2024 on everything -- I could look at software and understand why it was increasing or decreasing, the same thing with the infrastructure. On the professional services it wasn't as clear to me how it was $1.1 million less in 2024, which is a good thing normally, but I was trying to under -- I couldn't really tell where those cuts were coming from. I could see what made up the total, but not really how, I think on one of the pages a couple of slides up there was a part you actually showed the $ 7.7 million and put in what that was. Part II of it didn't actually make sense to me because it said $197,000 and that was all of Part II that was there, but it doesn't tell me what the difference is. So, in other words, what are the things that came out of the number in 2023, what were you spending money on that you are not going to spend the money on because it's a 12 percent reduction which is pretty steep. It's good if you guys can pull that off, that's a nice reduction in the staff aug and professional services. So, you spent $1.1 million more in 2023 or you are planning to. What is it that you are not spending that causes that reduction? So, there wasn't quite a good bridge on it.

**Aditya Gavvala:** Yes, sure. So, let's go back to slide number -- can you keep moving back, go to the right slide.

**John Vaughan:** One more back, one more back.

**Aditya Gavvala:** Yes, page number 5. Let me explain the difference in professional services and staff augmentation. In year 2023, in this year the bulk of the spend was on staff augmentation. We had about 32 contractors in this year because we had some major initiatives that we had to accomplish this year. That includes testing our systems for a 450,000 claims event, which you saw in Robert's report, so we needed to hire performance testing staff to complete that scenario planning event that we were doing before the beginning of the CAT season. We had some major initiatives, like we implemented a fraud analytics system, so we hired some contractors to complete that work. We also delivered electronic policy document delivery to our policyholders, so we hired contractors to complete that work. All that work wrapped up this year. Next year, we have three major flagship projects, Eligibility Reimagined, our Citizens Insurance Suite migration to the cloud, and our Enterprise Litigation Management where we contracted with the vendors. The Vendors are providing services for that, so we didn't see a need for continuing staff aug on those flagship initiatives. That led to a significant reduction in the contingent staff between 2023 and 2024.

The reason why you see Part II as a smaller number and Part I as a bigger number is because some of the contractors that we have are going to continue. We will not have 32 contractors, instead we will have 18 contractors supporting the in-flight initiatives and the other initiatives that are planned for next year. Those contractors are already in place, and they will continue from January throughout the year. That's the reason why you see a shift in dollars in Part I. Part II is any spend that we would incur from May onwards. That's why you don't see Part I as a significant number.

Additionally, we have to pay for the Gartner subscription and some of the other subscriptions that are also bundled in our professional services, those are in Part I.

Does that answer your question, John?

**John Vaughan:** Yes, to recap what I got out of it, it really had to do with the staff augmentation. You are cutting that by quite a bit in 2024, and the ones that are continuing are all budgeted into the Part I piece of the equation --

**Aditya Gavvala:** Yes.

**John Vaughan:** -- which is why part two looks smaller.

**Aditya Gavvala:** Yes.

**John Vaughan:** Some of those were in Part II of 2023.

**Aditya Gavvala:** You got it.

**John Vaughan:** Got it. Yes, that works. Thank you.

**Chairman Butts:** Great. John, anything else? Good. Any other questions? Perfect. Aditya, do you want to go ahead and read the action item?

**Aditya Gavvala:** Yes, sir. Staff proposes that the Information Systems Advisory Committee review and if approved, recommend the Board of Governors authorize the Technology Infrastructure, Software, and Professional and Staff Augmentation Services - Part I contracts for an amount not to exceed $24,547,149 as set forth in this action item, and authorize staff to take any appropriate or necessary action items consistent with this action item.

**Chairman Butts:** Thank you. We will entertain a motion to accept the action item[1] as read.

**Technical Advisor John Vaughan a motion to approve the Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Park I Action Item. Governor Nelson Telemaco seconded the motion. All were in favor, and the Action Item was unanimously approved.**

**Aditya Gavvala:** Thank you very much.

**Chairman Butts:** Thank you for the presentation as well.

## 5. New Business

**Chairman Butts:** Moving on to new business. Any new business? Seeing none, we will adjourn the meeting for today. Hope everybody has a great day.

**Kelly Booten**: Thank you.

**Chairman Butts**: Thank you, take care.

(Whereupon the meeting was adjourned.)

[1] Verbatim correction: Stated as motion.