CITIZENS PROPERTY INSURANCE CORPORATION

Summary Minutes of the
Information Systems Advisory Committee Meeting
Tuesday, September 17, 2023

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened via Zoom webinar on Tuesday, September 17, 2024, at 10:00 a.m. (ET).

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

Jamie Shelton, Presiding Chair
Joshua Becksmith
John Vaughan
Aditya Gavvala, *staff*

The following Citizens staff members were present:

Barbara Walker	Joe Martins	Tim Cerio
Bonnie Gilliland	Mathew Carter	Wendy Emanuelson
Eric Addison	Raina Harrison	Wendy Perry
Jay Adams	Ray Norris	Yuliya Rogatcheva
Jeremy Pope	Sarai Roszelle	
Jessica Chapman	Sudheer Kondabrolu	

Chairman Butts was unable to attend today's meeting today. Governor Shelton filled in as presiding chair. Roll was called and a quorum was present.

1. Approval of Prior Meeting's Minutes

Presiding Chair Shelton: Thank you, Wendy. Welcome, everyone. Thanks for being here this morning. We'll jump right into the meeting, and everyone should have the agenda available to them.

First item will be approval of prior minutes from the March 26th meeting. I know we've had a chance to look at those. Chairman Becksmith, I'll entertain a motion from you to approve.

Governor Joshua Becksmith made a motion to approve the March 26, 2024, Information Systems Advisory Committee (ISAC) Minutes. Presiding Chair Jamie Shelton seconded the motion. All were in favor and the minutes were unanimously approved.

Presiding Chair Shelton: Next item, the ISAC Charter for the annual charter review. I'll turn it over to Aditya; you are recognized to present.

2. ISAC Annual Charter Review

Aditya Gavvala: Hello. Good morning, committee members and folks on the call. The first item on the agenda is the ISAC minutes -- sorry, the ISAC annual charter review. There haven't been any changes to the charter since last approval. We have the annual review cycle with this one, so

it's coming back to this committee for approval. No changes have been made since last approval. So, I would like to request the approval of this charter today.

Governor Joshua Becksmith made a motion to approve the Information Systems Advisory Committee (ISAC) Charter as presented. Presiding Chair Jamie Shelton seconded the motion. All were in favor and the motion carried.

Presiding Chair Shelton: Aditya, you are recognized for the next action item, which is the strategic plan.

3. IT Strategic Plan Update

Aditya Gavvala: Thank you very much. I would like to share the IT Strategic Plan with the committee members today. This is an informational update for the committee.

Beginning with the first slide, this is where we state the IT vision and mission in alignment with the corporate vision and mission statements. What you see on the left-hand side on this slide is the corporate mission and vision statements. I'm just going to read it here as displayed on the slide: "We serve the people of Florida as the state's insurer of last resort, and as an innovative thought leader focused on promoting a healthy property insurance market." That's our mission statement – the company mission statement. And the vision statement is, "We strive to promote access, stabilization, and market competitiveness for Florida consumers, carriers, investors, and the overall property insurance industry."

Aligned with these mission and vision statements, we created IT mission and vision statements, which you see on the right-hand side. As stated here, "We provide and support secure, reliable, and dependable technology infrastructure, and deliver high-quality business solutions and data analytics to our internal and external customers." That's our mission statement. And vision statement is, "We will relentlessly drive value to our customers through highly engaged, responsive, and customer service-oriented IT workforce." Next slide.

We show the thought process behind our strategic plan. Our strategic plan is constructed with these building blocks that you see on this slide. At the bottom of that slide deck, you see the business goals. That's the foundational building blocks, which is what we used as a source to arrive at the strategic plan. Aligned with the business goals, we identified the key business capabilities and IT capabilities that are essential to support those business goals, and then, we used each of the pillars that you see here -- IT Principles, Enterprise Risks, Technology Trends, and Business Initiatives -- as the beacons to arrive at our strategic plan.

On the next set of slides, I will walk through each of these building blocks and the components of these building blocks, beginning with business goals. Next slide.

These are the three strategic imperatives for Citizens: Depopulation, customer experience, and emergency assessments. Our depopulation business goal is to promote depopulation and optimize access to the private market. Customer experience is to understand and enhance customer experience by regularly soliciting feedback, gauging the satisfaction, and optimizing our service capabilities and touch points. Emergency assessment, our goal is to reduce or eliminate the risk of emergency assessments. These are the strategic imperatives for the company.

On the next slide, you will see the key fundamental business capabilities that are essential to support these business goals. I'm not going to read through each of these, but they are listed for your convenience here. For example, for depopulation, it's important for us to have the ability to forecast the markets, access to the markets, and integrate with the markets. Those are some examples of the building blocks that are essential to achieve that business goal.

Likewise, for customer experience, the ability to provide omnichannel support -- that is support through different channels, email, phone calls, et cetera, and customer feedback management – those are some examples of the key business capabilities that are required to achieve customer experience.

Likewise, emergency assessments require us to have a strong product development team and the ability to assess the risks and analyze the risks and claims management optimization, and so on and so forth.

On the next slide, we show you the key IT goals. IT also has two key goals, and most of the work that IT does is aligned to these goals, in addition to supporting our business goals. The first one is Operational Excellence. The goal is to run the business operations that are cost optimized, resilient, compliant, and risk-managed. And the Reduced Risk IT goal is to protect IT systems and infrastructure against security threats. Next slide.

For each of the pillars that you saw previously, I'm going to walk through what each of those pillars are. These are the set of IT guiding principles used by IT for all decision-making. These are the six beacons that guide our decision-making process.

The first one is the Alignment. Everything that IT does must ensure that it aligns with the key business goals. That's the alignment principle.

The second principle is IT collaborates with key technical and business stakeholders in all decision-making. So, IT does not make decisions in a silo.

And third principle is IT aims to provide maximum long-term benefits to the enterprise. There has to be enterprise value behind what IT does. That's No. 3.

No. 4 is Fiscal Prudence. All investment decisions made by IT are fiscally prudent and comply with the procurement rules.

No. 5, IT decisions are governed through a formal IT governance process that balances risk and value.

No. 6 is compliance. We operate in compliance with all applicable laws and regulations.

So, these are the guiding principles that IT uses.

On the next slide, you see the key strategic risks identified by the office of insurance audit team working in collaboration with the executive leadership team. These are the risks identified as the 2024 strategic risks by the organization. So, they are listed here. Some of these risks have high rating and some have medium and low. This slide shows what we do within IT to help reduce these risks. Some of the strategies that you'll see will mitigate these risks.

Next slide we show some of the technology trends that we have used as a guide to craft our strategies. Two popular sources are used. The first one is InfoTech, a company that has specialized in this area. They share the technology trends each year with us, so we looked at the popular technology trends from that source. As you can see, the emerging trends are AI, robotics process automation and intelligent process automation. Transformative trends are cloud computing, cybersecurity, and Niche trends are internet of things, drones, mixed reality, et cetera, Entrenched are on-prem servers.

On the right-hand side, we also use another popular source that is geared towards insurance carriers. It's called Datos. We use the top tech priorities as identified by the Datos research in each of the areas: Agent and Customer Access, Business Intelligence, Analytics, AI, et cetera.

Next, we identified the key IT capabilities that are essential to support the business goals. What is listed on this slide are groups of those capabilities, popularly called capability domains. There are eight capability domains. Under each of those capability domains, there are a set of capabilities. IT went through a workshop identifying the key capabilities that are essential for supporting the business goals and prioritizing those capabilities, and that led to the strategies. The mapping of capability domains to capabilities is listed in the appendix for your information.

Next slide brings everything together, all these building blocks, and how the IT strategies are crafted together. On this slide, on the left-hand side, you'll see that we have the three business goals -- depopulation, customer experience, and emergency assessments -- and the two IT goals -- operational excellence and reduce risk. From those business goals, we identified the key business capabilities and IT capabilities that are required to support those, which is what the arrows point out. From there, we looked at all the different business initiatives and IT initiatives that are identified by the organization that are mapped to each of these business goals and we looked at the IT capabilities that are needed to support those business goals and business initiatives, arriving at the fourteen IT strategies that you see on the right side. They are color-coded to identify which business goal they actually support. For example, depopulation has a blue color, and you see the data warehouse modernization strategy supports that business goal. Similarly, reduced risk has green color, and you see that there are four strategies identified that support that particular IT goal.

That's the end of the slide deck. I have appendix material, and I'm just going to browse through them for your information.

The first slide in the appendix shows how business goals are mapped to different business capability domains.

On the next slide, this is the one where it shows business goals to business capability mapping.

On the following slide is an example of what a strategy on a page looks like. For each of the fourteen strategies, we will develop a strategy on page that looks like this. This is just an example to give you an idea of what a strategy on a page looks like.

The next five slides show how each of those business goals are deconstructed to business initiatives. From there, they are mapped to a corresponding IT strategy. This is an example where you have depopulation, which maps to three business initiatives that are in flight, such as loss history reporting, Citizens Reimagined, Exposure Reduction Program, which requires the key IT strategy, which is the data warehouse modernization.

And the next set of examples are for other goals.

That concludes my presentation today. I'll take any questions on the strategic plan at this time.

Presiding Chair Shelton: Are there any questions either from staff or anyone joining or Governor Becksmith?

Okay. Hearing none, we'll move on to the next item on the agenda, IT Security and Risk. This is Mr. Newman. I don't see you here, but I'm sure you're there somewhere. Wendy?

Wendy Perry: I don't believe he's been able to step away from the meeting he's in, but Wendy Emanuelson is on the line.

Presiding Chair Shelton: Okay. Well, then, Wendy, since it is both you and Brian noted here on the agenda, you're recognized to present the IT Security, Risk, and Resiliency Update.

4. IT Security, Risk & Resiliency Update

Wendy Emanuelson: Okay. Thank you very much. Good morning and thank you for your time today. I'm going to take you through the IT Security, Risk, and Resiliency updates.

It's very important to understand that organizational attack surfaces have rapidly expanded due to the increased use of software as a solution, digital supply chain, social media presence, custom apps, and then remote work and online customer interactions. Our core mission is to protect Citizens' data by ensuring integrity, availability, and confidentiality, and we achieve this by understanding our threat landscape. Next slide, please.

Understanding Citizens' threat landscape is crucial, and security is a repetitive process, continuously asking and answering these four basic questions: What makes us attractive to an attacker? What are we trying to defend against? What's happening in our world? And what do we need to protect? Those things change from time to time, but one thing to understand is we deal with a lot of chaos in what we do, and that's when attackers like to hit. They love chaos. So, we're constantly watching what's going on. Next slide, please.

The mission of the security risk and resilience team is to educate, advise, and empower our workforce to make informed cyber risk decisions and partner with internal and external teams to make Citizens' operating environment safe, secure, and resilient. As you can see here, these three objectives were introduced last year. They're the 2023-2025 objectives.

There were three key themes that drove our success here. First was divide and partner. With our small teams, cross-functionality was crucial. We collaborated closely with the business, with IT, and within our own functions -- the security ops, the GRC, and enterprise resiliency -- to achieve our goals. We measure to improve. We can't measure what we can't see, so metrics presented later in this deck highlight our progress over the past year, along with some historical data. Continuous improvement is the third theme. We focus on learning from both our successes and our mistakes and to avoid repeating history. Next slide, please.

Objective 1 was to establish a collaborative environment that leverages the expertise and capabilities of this multifunctional team and develop a comprehensive program that supports Citizens' overall strategy and enhances its resilience. This was developed based on the merging

of the enterprise resiliency team and the security teams, and we have achieved what we set out to accomplish.

In 2021, we began standardizing our security engagements by identifying value-added services and reducing bottlenecks. Through repeatable processes, proper training, and transparency, we reduce the lifespan of security engagements. And this is crucial because our small team must ensure early involvement in projects and integrate security controls from the start. It's much easier to put the controls in from the beginning than to retrofit. So, this also avoids delays and the perception that security is a blocker. Next slide, please.

This chart shows that lifespan of this objective. In the first two years, we identified support areas, defined engagements, and developed a run book that the team has continually revised and improved. With the objective achieved, continuous improvement will continue. You can see here on the right, the security support engagements. They include contract reviews with vendors, information security standards assessments, project support, project implementation support, questionnaires, et cetera. There's a list there. Some of these can live longer, but you can see we are down quite a bit over the last year, just 58.9 percent reduction in that lifespan. So, we're making improvements on those processes and streamlining them to get the same results in a shorter period of time. Next slide, please.

Objective 2 is to provide a systematic and proactive approach to identifying, assessing, mitigating, and managing IT risk and threats while proactively safeguarding Citizens' critical assets and data from potential threats.

On the next slide, you will see that in 2020 we began improving response times and remediation of risk and audit issues. The previous risk management tool was inadequate and lacked transparency. In 2021, we implemented a new tool with self-service functionality. It automated our workflows and made accessible dashboards, giving risk owners control and transparency. Since then, Citizens has significantly reduced remediation times, so 30.9 percent for audit issues and 64.8 percent for risk issues just in the last year. That's an 87.6 percent and 95.5 percent reduction over the last four years, respectively, with these process improvements. This success is due to the dedication of risk owners, the collaboration across teams, and the new tool's enhanced visibility. Most of the work -- don't get me wrong, most of this work is done by IT; however, the ability to give them a tool that automates the workflows, keep track of what they're doing, assign tasks, has been pivotal in reducing the time to remediate. Next slide, please.

In 2023, we began selecting a new managed detection and response vendor to enhance our security monitoring. Key criteria included transparency, improved communication, tool integration, and faster response time. We chose Ontinue, which met all our requirements. The program kicked off in March of 2024 and the new MDR is fully implemented, and we are already showing significant benefits. Ontinue is a five-time Microsoft Gold Partner and award-winning MSSP, which is a managed security service provider, and has delivered immediate improvements in our triage time for overall security operations. As you can see here in the first slide, on the top left, it's in that circled area, around March 17th, prior to that, we were averaging about a four-day time to triage incidents, and you see it kind of dropped down to nothing. It didn't drop down to nothing. We changed over to Ontinue and it went to minutes instead of days. As you can see in the time to triage, percentiles were low in the matter of minutes averaging, which is a great improvement. Next slide, please.

As discussed on the last slide, in 2023, we decided to switch from our existing managed detection response provider. They also supplied our security information event management system. That's

where we get all the logs from all our assets, all tools, et cetera. All those logs and alerts come in from that tool. So as a Microsoft-centric company, we've piloted Microsoft Sentinel SIEM, and which offered seamless integration with our existing Microsoft Azure tools. Sentinel supports ongoing activities like insider risk, user behavior analytics, DLP you heard Aditya mention earlier, and threat hunting, and it is enabling a more proactive approach to our threat landscape. Next slide.

So, I just covered two areas that are part of our overall Citizens' security layers. In this image, you see an illustration of Citizens' security layers, and on the bottom left side and the bottom right side, you'll see sort of a shell. There you'll see the activities of the security team: Policy management, which includes risk management, security governance, system assessments, security policy and compliance. Those things guide some of the work in the other layers that are going on. Then monitoring and response, that's our SIEM solution - IT service management, security operations, digital forensics, incident response and reporting, and detection and response, all of those things feed information coming from the rest of the layers. You've got the human layer, the perimeter security, our network security; our endpoints - those are all of the servers, the laptops, all of those devices; application security and data security, all of that feeding into the monitoring systems, and this makes up our Citizens' security layers. Next slide.

And, finally, for Objective 2, how are we doing? With all those layers, with all these changes that we're making, here's our progress. Since 2018, Citizens has been participating in Gartner's annual security assessment. While 2024's results are still pending, those are going on as we speak, this chart shows 2018 to 2023 against the industry benchmark. So, the industry benchmark is the red line, and we are the blue line. You'll see this assessment evaluates our Security and Risk Management program across seven objectives and 30 key activities. The details of those seven objectives and 30 key management activities can be found in the appendix for this slide deck. As you can see here, we've reached about 4.25, which is a good point and a quarter above our industry benchmark. Next slide.

We'll move on to the last objective, and that is to continue to improve the organization's resiliency and the ability to respond to any unexpected adverse events that might impact the business. So how do we do that? Next slide, please.

Understanding that resiliency planning is a life cycle, we start out with business impact assessments, technical impact assessments, and that's not a small feat. This is where we go out to every business unit and talk about the processes, their technology, and the people needed to complete those tasks. That is all documented. That information is then used to develop our business continuity and DR planning. It's also used to train staff to be able to respond using those business continuity plans and disaster recovery processes. Then we exercise those plans and those processes to make sure that we have the accurate and usable recovery time objectives and recovery point objectives, and they perform these in various ways. Those also help us determine a gap. You know, are there any gaps? Based on what the committed recovery points are, are they accurate? Should we make change? Then we update those plans and the cycle begins again. I just wanted you to understand that. Now, this used to all be done manually. We just recently purchased a tool, added to one of our other tools -- and if you could go to the next slide -- we are now doing this within the tool. The business impact assessment has begun. Here you see just a brief show of where we are with those business impact assessments. Some of them are in draft and review. This has changed a lot since this report has been done. We're probably a very higher number, but we're going to each individual business unit, each division, each business unit, and understanding what their process is.

What this does for us, though, is it changes everything. This allows immediate updates when technology services and personnel change, keeping our business continuity plans current. So, in time of need, we can now access those recovery objectives directly and see how process changes impact another process or impact the number of people needed, that type of thing, or technology. It also helps us to better plan by identifying dependencies up and downstream on technology assets as well. So, if technology needs to go down to update something, we can immediately see what processes are impacted and if other assets are impacted. Utilizing what's already existing out there, the IT department and CMDB, that's their configuration management database as well, it all links together.

This is how we preview a graph from our new tool. This is part of the dashboard. It shows that progress. Once we get all of this done and train the users to make real-time changes, the processes are then linked to the relevant technology assets and other processes and inform the business continuity plans, the disaster recovery requirements, and the exercises to identify and address gaps.

This is all I have for you today. I'm happy to answer any questions you may have. I know I covered a lot.

Presiding Chair Shelton: No, good presentation. Any questions for Wendy from staff, other governors, or anyone else on the call?

Governor Becksmith: No. I would like to say just one thing, Governor Shelton. I think the team at Citizens, the whole IT team and the legal team, have done a really thoughtful process through IT resiliency and through the safeguards. I know we all are seeing it on the news and kind of hearing about the IT security and cyber-attacks and everything and taking this stuff very, very serious, and I just want to compliment the entire team on behalf of the board of governors and the job they've been doing. So, job well done.

Wendy Emanuelson: Thank you.

Presiding Chair Shelton: Thank you, Governor. Thank you, Wendy. Anyone else? Okay. Hearing none, we'll move on to the next item on the agenda. Aditya, we'll go back to you for -- we have an action item, our Technology Infrastructure, Software, and Professional and Staff Augmentation Services, Part 1. You are recognized.

5. Action Item

a. Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part 1 [AI]

Aditya Gavvala: Thank you, Governor. I would like to draw your attention to the slide deck on this particular item. I would like to provide some context before we go into the action item. Beginning with the definitions here, this action item is a request for spend authority for a collection of IT items that are procured through state contracts, GSA, or through alternate government-approved contracts. There are two parts to this action item. The first part is primarily focused on IT items purchased between January through April of 2025, and that's what is coming to the committee today for approval. And then, Part 2 is for any IT items that are procured from May through December of 2025. This will come to the December ISAC committee at that time, but our focus today is primarily on Part 1.

There are three categories of IT items that are included in Part 1, which are infrastructure category -- that's primarily any technology hardware, network infrastructure, telephony, connectivity, data centers, storage, et cetera -- and the second category is for software and third category is for professional services and contingent staff.

On the next slide, on the left-hand side, you see the total for Part 1 and Part 2 and the composition of the total. Part 1 is a total of $25.162 million. Part 2, which is just an estimate at this time, when we bring the Part 2 action item to the board in December, it'll be refined, but at this time, we estimate that to be $4.383 million.

In the middle, you see how those dollars are divided between infrastructure, software, and professional services and staff augmentation. As you can see, the infrastructure total for Part 1 and Part 2 is $3.68 million; the blue bar shows what is in Part 1 and the orange bar shows what is in Part 2. Similarly, in the middle, you see software, which has a total of $18.1 million. Part 1 is $14.292, and Part 2 is that orange bar up at the top. And professional services and staff augmentation predominantly is in Part 1.

On the right, you will see Part 1 and Part 2 separately broken down by software, infrastructure, professional services and staff aug. So, for Part 1, the total is $24.162, of which $14.292 is software, $3.174 is infrastructure, and $7.69 million is actually professional services and staff augmentation. Let's go to the next slide.

This slide shows you the details behind Part 1 and Part 2 in a tabular format. It puts things in the right perspective and compares it with what we had for last year. Three categories. Each row here represents the category: Infrastructure, software, professional services. Then you have three sections on the table. The left section is for Part 1, the middle section is for Part 2, and the right section is the totals.

As you can see towards the right, for 2024, both Part 1 and Part 2 combined total was $32.58 million that was approved by the board. And what we estimate for 2025 is $29.5 million, which is $3 million less than what we had for 2024. Now, focusing on Part 1 alone, which is the left section of that table, Part 1 for 2024 was $24.5 million. For 2025, we are seeking $25.1 million, which is marginally higher, about $615,000 more compared to last year, but the savings are primarily in Part 2, which is going to come to board in December. For 2024, Part 2 total was $8.03 million. We estimate for 2025, Part 2 to be $4.38 million, which is $3.6 million under. That's where the savings come from.

The next slide takes a deeper look at Part 1 and Part 2. The table on the left-hand side compares 2024 Part 1 with 2025 Part 1, and the bar graphs on the right side compare 2024 Part 2 with 2025 Part 2. There are three colors here. The orange color represents infrastructure. As you can see in Part 1, there's a significant reduction in infrastructure for 2025 compared to 2024, and those reductions come from a couple of things. We are getting rid of some of the legacy telecom equipment. We implemented a modernization project this year. We took our telephony to the cloud through the Unified Communications and Contact Center as a service implementation that was approved by the ISAC committee and the board. That reduces $1.47 million spent on the legacy telecom. We also refreshed our firewall and network infrastructure in 2024. That's not needed for another three to four years. So that leads us to a $2.18 million reduction. Through the cloud migration project over the last three years, we migrated the majority of our production systems to the cloud, and starting from the beginning of next year, we will be reducing our footprint in our

primary data center here that is leading to a cost saving of $670,000. So net result is that $4.32 million reduction in infrastructure spend compared to 2024.

Software category, on the other hand, which is in the yellow color, in Part 1 is going up. That's largely due to a multi-year purchase that we are making in 2025. It's hitting the books in 2025, but that covers for three years, 2025, '26, and '27. That's the Microsoft end-user license agreement for $6 million. While it appears like our software spend is going up, it actually covers three years. That's why you see that looking higher. Similarly, we are also purchasing portal and media platform software for three years; it's hitting the books in 2025. That's $690,000 for three years. That's what is giving the appearance of software actually going up, but in reality, software is actually more or less the same or less than what we had for 2024.

In the area of professional services and staff aug, we are actually shrinking. The net total is reducing by $388,000 because some of the implementation services are concluding in 2024 and not needed for 2025. That's the $388,000 savings.

That's the conclusion of the slide deck. If there are any questions, I'll take them before I go to the recommendation, Governor.

Presiding Chair Shelton: Thank you. I won't speak on behalf of Governor Becksmith, but it's important, I think, to note -- and something we talked about when you and I went through this ahead of time -- we as governors and board members, the oversight to which we have, the amount of dollars you're talking about spending, the different types of projects, software, hardware, augmentation -- all the -- you know, to say that's beneath me, it's beneath me because I don't know all the needs that you have in the organization. And as you recall, one of the things I asked and you provided for me and for all of us is that, you know, what is the spend that we do relative to our peers and what is a way of measuring that benchmark data against insurance companies like us? And you provided that to me earlier on, and we are well within and even slightly below in a lot of cases what we're spending to keep up and do this service not only to our customers, but to our employees to make sure everything is running well. And I just want to make sure that's pointed out that we do look at it from that perspective besides all the work that you and your team put in. And great job, and I don't have any other questions or comments. If there's any from Governor Becksmith, he will certainly weigh in, and if there's not, then anyone else have any other questions? Okay, then. Go ahead -- there's an action item you want to present?

Aditya Gavvala: Yes. Before we go there – thank you, Governor, for reminding me about what we discussed -- I would like to share this with the committee today. I have included a slide in the appendix. Raina, if you don't mind going back to the last slide in the appendix? Yes, that one right there. The one that --

Presiding Chair Shelton: There it is.

Aditya Gavvala: This is a good slide that puts things in perspective for us. You asked a very, very valid question about IT spend for Citizens, how does that compare to industry? And this is a slide that actually compares us with the industry benchmark. There is a popular benchmark that most of the insurance carriers use. That is from a source called Datos, and the link is shown on the right-hand side. Let me walk through this graphic. Each of the bars represents the total direct written premiums for Citizens Property Insurance for each year. In 2024, our total direct written premiums are at $7.1 billion. This is projected numbers from the beginning of the year, right? At this time, it might be lower because of the depopulation program that's been really successful, but this was

created at the beginning of the year. At that time, it was $7.1 billion. And the gray line there shows what other insurance carriers are spending on IT. They are spending 4.2 percent of the total direct written premiums on IT. That's the industry benchmark. Compare that to our orange line, which shows we are only spending 1 percent, our IT budget is 1 percent of the total direct written premiums. So, that's significantly under what other insurance carriers are spending.

In order for us to be at 4.2 percent, our total direct written premiums need to shrink down to $1.57 billion. If we depop that much of our business, then our IT spend would be in alignment, so we're significantly under compared to other insurance carriers.

I thought this was a good slide to show you and share with the committee members today.

Presiding Chair Shelton: Thank you for sharing that. Any other questions? Okay. We'll move on to your action item.

Aditya Gavvala: Yes. Thank you. So let's go to the "Recommendation" section, which I'm going to read here for committee members: "Staff proposes that Information Systems Advisory Committee review, and if approved, recommend the Board of Governors: A) Authorize the Technology Infrastructure, Software, and Professional and Staff Augmentation Services Part 1 contracts for an amount not to exceed $25,162,832 as set forth in this action item, and B) Authorize staff to take any appropriate or necessary action consistent with this action item."

Presiding Chair Shelton: Well, being that it's myself and Governor Becksmith to move this along to the board, I will ask if Governor Becksmith would propose a motion to approve this, and assuming he does, I will second it and we will move it along. Governor Becksmith?

Governor Joshua Becksmith made a motion to approve the Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part 1 Action Item. Presiding Chair Jamie Shelton seconded the motion. All were in favor, and the Action Item was unanimously approved.

6. New Business

Presiding Chair Shelton: I don't see anything else on the agenda for this morning except the little placeholder that says "new business." Is there any new business from anyone on the call today or part of the group they'd like to present or bring forward? Hearing none, thank you, staff. Thanks, everyone. Great, great presentations. Good seeing you again, and we'll see everyone next week in Lake Mary.

Thank you.

(Whereupon the meeting was adjourned.)