Information Systems Advisory Committee September Minutes

☒ **ACTION ITEM**

☐ **New Contract**

☐ **Contract Amendment**

☒ **Other - Committee Minutes**

☐ **CONSENT ITEM**

☐ **Contract Amendment**

☐ **Existing Contract Extension**

☐ **Existing Contract Additional Spend**

☐ **Previous Board Approval**_____

☐ **Other**_____

Action Items: Items requiring detailed explanation to the Board. When a requested action item is a day-to-day operational item or unanimously passed through committee it may be moved forward to the board on the Consent Index.

☐ **Move forward as Consent**: This Action item is a day-to-day operational item, unanimously passed through committee or qualifies to be moved forward on the Consent Index.

Consent Items: Items not requiring detailed explanation to the Board of Governors. Consent items are contract extensions, amendments or additional spending authorities for items previously approved by the Board.

Item Description	Information Systems Advisory Committee Meeting Minutes September 8, 2021
Purpose/Scope	Review of the September 8, 2021 Information Systems Advisory Committee Meeting Minutes to provide opportunity for corrections and historical accuracy.
Contract ID	N/A
Budgeted Item	☐Yes ☒No - Not applicable
Procurement Method	N/A
Contract Amount	N/A
Contract Terms	N/A
Committee Recommendation	Staff recommends the review and approval of the September 8, 2021 Information Systems Advisory Committee Meeting minutes.
Contacts	Kelly Booten, Chief Operating Officer

CITIZENS PROPERTY INSURANCE CORPORATION

Summary Minutes of the
Information Systems Advisory Committee Meeting
Wednesday, September 8, 2021

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened via Zoom webinar on Wednesday, September 8, 2021, at 9:00 a.m. (ET).

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

Nelson Telemaco, Chair
Lazaro Fields
Brian Foley
Kelly Booten, staff

The following Citizens staff members were present:

Aditya Gavvala
Barbara Walker
Barry Gilway
Belinda Miller
Carlos Rodriguez
Christine Ashburn
Eric Addison
Jennifer Dilmore
Ray Norris
Robert Sellers
Sandy Allison
Sarah Harrell
Stephen Guth
Tim Cerio
Wendy Perry

Call Meeting to Order
Roll was called. Chairman Nelson Telemaco, Governor Lazaro Fields, and Technical Advisor Brian Foley were present. Chairman Telemaco called the meeting to order.

1. Approval of Prior Meeting's Minutes

Chairman Telemaco: Welcome everyone to the September 1st ISAC meeting. Our first order of business is the seeking approval for the prior minutes. Do I have a motion?

Governor Lazaro Fields made a motion to approve the September 8, 2021, Information Systems Advisory Committee (ISAC) Minutes. Technical Advisor Brian Foley seconded the motion. The minutes were unanimously approved.

Chairman Telemaco: Next on the agenda is Kelly Booten. I'd like to recognize her to provide the Chief Operating Officer Update.

2. Chief Operating Office Update

Kelly Booten: Good morning, Governors. Kelly Booten, for the record. Today, I would like to provide an overview of a dashboard that we've created. Next slide, please.

At Governor Telemaco's, request we've created a dashboard that provides a snapshot of IT health encompassing many of the objectives of the Committee as stated in the Charter. We will

continue to revise the dashboard to meet the expectations of the Committee and welcome your feedback.

In the upper left quadrant, we capture the IT Financial snapshot with a focus on this year's budget, projections, and actuals. Although projections are captured in the system on more of a quarterly basis, actuals are compared to budget on a monthly basis with budget variance commentary for each category. At this time, there are no budget concerns, and we are projected to be under budget for the year.

In the upper right corner, we capture, at a very high level, execution of strategy and progress according to the four phases across the top: Develop Strategy, Architecture and Planning, Procurement, and Delivery. The strategies tie back to the IT Strategic Plan, which Chris Jobczynski presented at the last meeting, and are color coded to this year's Key Strategic Themes. To the far right is an indicator regarding the health, on target or not, and all strategies are currently on target. Underneath most of the strategies are many projects with more detailed reporting, and many of these strategies and associated initiatives will be covered in future meetings via status updates or action items. Today, the Application Integration Platform Action Item is being presented by Aditya Gavvala and the Identity and Access Management by Sarah Harrell.

In the lower left quadrant is a snapshot of Resiliency from a Catastrophe Readiness perspective and an IT Disaster Recovery Readiness view. This quadrant will ebb and flow with the time of the year, as the cycle starts every year after storm season where we reset the plan and monitor it to conclusion. Today, Robert is presenting more detail regarding this section.

In the lower right quadrant is a snapshot of IT Risk. We have kept this at a very high level as the risks themselves are sensitive and predominantly pertain to IT Security and cybersecurity-related topics. Sources of risks can be from independent audits, risk assessments, control attestations, penetration tests, employee reporting, and other means. All risks, risk mitigations, and risk acceptance is tracked and monitored. Today, Robert and Sarah will also provide additional information regarding this quadrant.

With that, I'll pause for any questions or feedback regarding the dashboard.

That concludes my report.

Chairman Telemaco: Kelly, I'm sorry, can you go back to the dashboard quickly, if you don't mind?

Kelly Booten: Yes, sir.

Chairman Telemaco: So, if I'm reading this correctly, the projections as of May are shy of the 2021 budget so we're in good shape there, and the IT Finance expenses through June is less than half of the projection, and the budget for that matter, is that correct?

Kelly Booten: That's correct.

Chairman Telemaco: Excellent. And then on the bottom right, the IT Security Risk Profile. The medium risk is going up, but the high risk is going down. As the medium risk goes up, do we

worry about any of that going into the high or is it that the high-risk levels have dropped down into the medium bucket?

Kelly Booten: Great question. The high has changed, and we've mitigated the risk sufficiently so that the high was downrated, so to speak, to a medium, and that caused the medium to go up. So, it was a movement from the high category to the medium category. Notice to the left, there's a mitigation effort, and we've got that on target. There's mitigation under each one of these risks that we monitor and track. There's also oversight from our Office of Internal Audit in managing our risk and the Risk Steering Committee at Citizens.

Chairman Telemaco: Excellent. So, it looks like we're on target and below budget, which is awesome. Any questions from any of the members on that report? Okay, great. Thank you, Kelly, appreciate that.

We're going to move on to item number three on the agenda and I'm going to turn it over and recognize Robert Sellers for the IT Security, Risk and Resiliency Update.

3. IT Security, Risk & Resiliency Update

Robert Sellers: Good morning, Governors and Advisors. My name is Robert Sellers, and I'm the Chief Technology Officer for Citizens. Within my organization, the Director of IT Security & Risk, Carlos Rodriguez, is responsible for the strategic and day-to-day activities related to IT Security, our Incident Response, and our IT Security and Risk compliance management. Sandra Allison, the manager of Enterprise Resiliency, is responsible for our numerous Enterprise and IT Resiliency operational areas. Both of these individuals are here with us today, as well. These active and dynamic areas are on our IT front lines to ensure our operational capabilities remain available to meet the needs of our policyholders and other stakeholders.

As always, I'd like to remind you that individual, detailed briefings on our specific Security and Risk activities and our Resiliency activities with any of the Technical Advisors and Board Members are always available at your request. We have also provided, at the back of this portion of the presentation, a terminology slide that provides definitions for common terms and acronyms utilized in this particular discipline area. Unfortunately, there are many of those in the IT area and we've done our best to itemize those and provide context. Slide one, please.

I'd like to start with the Control Frameworks that we utilize here. This is really at the core of our Security Control Framework. We have chosen the Critical Security Controls, down there at the bottom, that were developed by the Center for Internet Security (CIS). They define the Top 20 controls that have been shown to mitigate most of the common and impactful security attacks and they have become a guide for many organizations that defines the specific tools that we use in our program for the different functions.

Program Framework: The second level is a security program framework, the second ring in the graph. It's like an architectural blueprint, and we utilize the National Institute of Standards and Technology Cybersecurity Framework. Big words, lot of words, but it's formally known as NIST and the NIST CSF. This defines five high-level functions for IT Security and Risk: Identify the risk, Protect the risk, Detect attacks, Respond to such attacks, and then Recover. By following that five-function process, we hit a number of different controls to ensure that we have each of the actions in place. Those five functions decompose the complex world of security into simple categories that model the high-level lifecycle of all our security activities that can be

communicated in a common business language. That's key because we're dealing with highly technical areas that we're really trying to communicate risk and the protection and the management of that risk out to a larger group of people. I'll talk a little bit more about that in a little bit. One reason that we chose this framework is it is widely adopted throughout most, if not all, the state agencies in Florida, and many other organizations around the world.

Risk Frameworks: Beyond the activities defined in the control or program frameworks, we also need a way to determine what capabilities we have to prioritize.

There are several frameworks that define approaches to risk assessment and management including NIST and ISO, COSO Enterprise Risk Management, among many others. That's one of the challenges. There are so many that we end up taking them and modifying them to be a good hybrid approach for Citizens. The IT Risk Management framework at Citizens, like the Enterprise Risk Management framework, starts with the Three Lines of Defense model that we'll see in action on the next slide; however, from a practical point of view, as I mentioned, we built a program that incorporates items from all of these that fits Citizens' needs. That's critical that we're focused on the needs that we have here. We have many external partners that help us with that.

Finally, we have an Enterprise Risk Management program based on the Three Lines of Defense and COSO, which also uses COBIT. All of these are control frameworks to guide the internal controls when it comes to IT, and those frameworks guide our priorities from an Enterprise Risk Management level.

So, again, in the Security and Risk space, it's not about choosing one framework. We've chosen a set of frameworks to mold an overall one for Citizens' requirements and to communicate with the Enterprise in a common business language while we continue to adapt our Security and Risk programs to, unfortunately, meet the constantly changing threat landscape. As y'all know in your own businesses, in your own personal lives, the threats are out there, they are continually evolving. Are there any questions on the Frameworks? Next slide.

Three Lines of Defense: As I mentioned, we utilize the Three Lines of Defense approach because of two reasons – one is that our Office of Internal Audit and Enterprise Risk also follows this model for managing risk across the enterprise, and second it helps us communicate that risk is a shared responsibility across the organization, and that everyone has a role in it. From the bottom up going left to right, we have the many ongoing operational activities that regularly take place. It highlights the roles and responsibilities of the operational teams, risk management, and the executives. Then at the very top and going down, you can see that our executive team sets the tone, our risk tolerances, and direction that we all put into practice through implementation of the frameworks, standards, and policies that govern our IT and our Security Program. In addition, we also have external stakeholders who, like our Office of Internal Audit, bring independent assurance to our program. Next slide please.

Strategic Objectives: When Carlos joined in 2017, early '18, we focused on building a strategic program for our security and risk. It's been very successful over the last three years, as I previously briefed the ISAC. This is a revised version for 2022-2024 for the upcoming period.

I'd like to cover, at a very high level, the strategic objectives for the IT Security and Risk Program. Consistent with the dynamic and broad nature of the area, we have objectives focused on people, processes, and technology. Since 2017, we've been focused, with our

partners across the organization, on improvements in our risk culture with our maturity and awareness improving every year. Controls and actions, such as lower levels of formal audit findings, increases in internal staff across the organization identifying risks and issues, and our timely treatment of such, are examples of this and some of what is demonstrated in the dashboard presented by Kelly earlier. With new risks seemingly appearing almost every day, each of these objectives, starting with an understanding of risk and how we manage it here at Citizens, is important.

You can see going down the right-hand side of the table that the descriptions next to each of these objectives and the dashboard's top technology strategies and theme alignment, that the level and type of projects and programs necessary to accomplish each of these objectives are numerous and large.

When we're taking action that affects potentially hundreds of technology systems across numerous data centers, a 1,000+ employee organization with 8,000 agents, a significant number of potential CAT and regular adjusters, and over 600,000 policyholders, this isn't a simple task. Identifying and targeting these objectives, our focus is clearly on managing the cybersecurity risks at the levels identified as appropriate for an organization of our size and with this level of responsibility.

As we go through this briefing formally next year and the year after, we will continue to focus primarily on this slide here and the actions and the steps that have been taken over the course of the past year, and the actions that are identified for the upcoming year, based on our budget, based on our risk management, and based on our priorities. Next slide please.

Ransomware: At the meeting last quarter, questions were asked about our posture on ransomware and some of our operational areas that could assist in guarding and responding to this threat, and for good reason. Ransomware's the fastest growing significant cybersecurity threat for many businesses and individuals today, and we wanted to give you a general idea of the controls that we're using to manage this risk at Citizens'.

On the left side of the table, you see a set of aggregated controls recommended by about 14 US Government Agencies, and how those recommended controls map to the objectives of our combined cybersecurity and resiliency programs. We have numerous audits and other verifications by outside parties and inside our organization to validate that these controls are in place and functional. We also, as part of our operational tempo, regularly review, formally test, and exercise the technology, our staff and management, and the third-party organizations that are involved in the five high-level functions I mentioned before.

Governors, to conclude this portion, please notice that I've left out any specifics on the technologies implemented in our environment. We have several rings of defense, some automated, some people focused, and I want to remind you that individual briefings are available to you upon request on this topic, or any other topic.

Are there any questions at this point on the Security and Risk area? If not, I'll move on to the Resiliency area.

Brian Foley: Yes, this is Brian. One of the fancy terms that's being thrown around these days, and I'm sure it's baked in your thinking here, is Zero Trust. You know we're migrating from an environment of "trust, but verify" by tracking credentials and logs, etc., to an environment where

we are hardening the perimeter, and hardening the inside access, as well, with this new industry notion called Zero Trust. So, I'm assuming you've thought about how that fits into this framework.

Robert Sellers: We have. I won't call it the hot topic because it has been around for a while, but it is gaining strength, gaining a priority for many organizations, including ours. As we're moving to the cloud, we're redeveloping certain capabilities in that area. But to your point, we looked at identity, identity being the new perimeter for organizations like ourselves, but it's much deeper than that. Ensuring somebody has the appropriate credentials to do what they need to do is only one small facet. The inside of the network, historically, has actually been a soft target for many organizations. We spend a lot of money and resources on protecting the perimeter, but who gets access to what on the inside by our employees? When should they have access, how should they have access, from what devices, where are they located geographically? All these things are part of the zero-trust model, and it is part of our consideration, Brian, as we move forward in maturing these areas.

Brian Foley: Thanks.

Robert Sellers: With that I'd like to transition over to Enterprise Resiliency. Next slide.

When we look at Enterprise Resiliency, it's basically our ability to anticipate and respond to negative situations. An unexpected crisis, the pandemic of 2020 and the impacts to us, a major storm hitting Jacksonville or Tallahassee and having an impact on our business operations, would previously have been a significant event, but today we're looking at other types of events, as well. The unexpected crisis of them, what is unexpected? Is it policy growth, is it other areas that fall into the categories where we need resiliency for the organization? So, as we move through this and start thinking about our resiliency activities, we've got five different areas that we focus on within this this group.

First, we focus on methodologies around our crisis and emergency management, some of which is very applicable to this component.

We think about business continuity. How do our business units continue to operate when they don't have a system or a place to work from?

IT, from a standpoint of resiliency, what happens when we have a system go down? What would happen if we had a major policy system or a financial system that went unavailable for some period of time? How would the organization work but, more importantly, how would IT recover that system back to an operational state?

We also think about third party and contingency management in the area of resiliency. In many cases we're only as good as our partners, whether it's our BPO partners in the underwriting area or claims adjusting organizations that support us in a CAT event. Those organizations - how do they manage their risk, and how do they recover from that? And how do we support them and how do we deal with it if they if they're not available?

And the final methodology that we follow and plan for is a CAT event itself, a major hurricane. How does IT respond to assist our claims partners and other organizational units that are responding to a claim event?

The Business Impact Analysis is a key component to this. It helps us focus on what's important, how we're going to deal with it, and then document and address the plan. Next slide please.

Quick summary - every one of our systems has a recovery timeframe that's part of our BIA. You can see systems that have to be recovered in eight hours, systems and organizational units that may not need those systems for anywhere up to 2-3 days, all the way up to +2 two weeks. These have been prioritized by the business for the recovery efforts that are necessary to continue the priority business for our policyholders and other stakeholders.

As we move to the cloud, obviously this is a dynamic area that is changing resiliency, recovery. Our capabilities in the cloud are significantly greater just by the fact that those capabilities exist there, for making some of these much less, in terms of time, to actually recover these systems, and will help to support these business units in their processing if we were to have an impact. Next slide please.

In 2021, we have a number of different governance processes. Most of this, if not all of it, is well documented. We have numerous stakeholders inside the organization, as well as outside, that look at our disaster recovery plans and business continuity. Whenever we go for reinsurance, they're definitely interested in how we're doing these programs. So, over time, these plans and documents have been built and distributed and shared within the organization and are now, in many cases, maintained by the organization itself, by the business units that have responsibilities for these. We do have an advisory committee that's made up of senior management inside the organization to assist in our prioritization and oversight, and we have a number of different programs that are running as part of our ongoing resiliency activities that are taking place this year. Next slide.

When we look at the continuity plans, you can see that we're right in the middle of the update activity that's going on in August and September crossing most of the different business units. Claims gets ahead of the curve to CAT season by redoing their stuff in February, otherwise we go through, and just validate with the different business units here in the August-September timeframe. Next slide please.

Claims Strike Zone: Just as a point of information, each year we do some testing. This year we utilized our third party, Agility Recovery Solutions, and actually executed. They brought the vehicles on site, we validated with our Claims organization the ability to set up a Mobile Recovery Center, and also operated with several of our business units, including our Mail Center, in this particular facility. That's been a very good partnership and provides us with this mobility capability, as well as physical structures in Jacksonville, Tallahassee, and other areas of the State. Next slide please.

Business Continuity: Our Business Continuity exercises are ongoing. These are desk exercises in many cases, working with the different units to take the programs that they have in place, review them, and in some cases that becomes the refresh cycle for that unit. In other cases, they go through the refresh and then we test it after they've completed that cycle. You can see the July through October timeframe is the hot period for this.

In 2021, we are running a Business Continuity activity that is focused around a cybersecurity incident. We intend to make that a real-world type of activity, an exercise that will build upon ransomware and other security threats that we have at this point and that we've identified. Next slide please.

IT Resiliency and Disaster Recovery: As I mentioned, one of our methodologies is focused on backup and recovery point objectives. The immutability of the data itself, which we're focused on, basically backing it up in such a way that it cannot be changed by ransomware or by other threats and actions that might take place. That's a key component to the ransomware threat model and response model.

The failover test in 2020 was performed against the primary insurance suite. In 2021, we focused on, not only the CIS suite, but a number of others. This was a failover from our Jacksonville Data Center to our Winter Haven Data Center. We'll continue with other tests throughout the year with telephony being the next major one. We have other quick statuses, down here at the bottom, of different systems and their readiness for recovery. Next slide.

Enterprise CAT Assurance: This is the area where we respond and assist the Claims organization in our responsibilities to manage a hurricane and our adjusting and other claims support activities. We finished our CAT assurance process in June with over 130 checklist items across the entire organization. We have a readiness for storm. We've had a couple here in the last couple months and, hopefully, that will be it, but we are ready if we're called to perform in that type of environment.

From an Enterprise Resiliency standpoint, we continue to focus on the availability and continuity of our operations and the technology to support that primary focus. Any other crisis identification, any risks that we identify in the organization that might need that type of treatment, we go through and build an appropriate plan, evaluate, and plan.

Chairman, that concludes my remarks today and the formal briefs on the Information Security & Risk, and Resiliency areas as required by the Charter.

Chairman Telemaco: Thank you, Robert, for the report, that was excellent. I'll open it to the members for any questions?

I've got a question if you go back to slide 10. That Citizens Business Impact Analysis process - I'm curious when it was conducted.

Robert Sellers: The last business impact analysis was performed in late 2019. Current for 2021 is underway at this time. We tend to do those every two to three years. The most important thing around the business impact is that when a business unit changes their processes, that they go through and update their continuity plan at that time. We have Continuity Champions scattered throughout the organization that are trained to focus on that.

Chairman Telemaco: Excellent. So, this will be refreshed in 2021…

Robert Sellers: Right.

Chairman Telemaco: It's constantly refreshed, but in 2021 there will be a concerted effort – okay, excellent.

And then on slide 12 where you have the maintenance schedule. There were some items that were highlighted in yellow as pending. I just wanted to make sure that there is no reason why those wouldn't be in process, especially those in September, now that we're already in

September. It's just that those dates haven't come, yet? There's no obstacle for that to end up being in process pretty soon, right?

Robert Sellers: That's correct. There are actions that are taking place on both of those at this time.

Chairman Telemaco: Okay, and then there's one on the following page that shows the Treasury & Investment as scheduled on September 1. Has that already started, is that in progress now?

Robert Sellers: Chairman Telemaco, I will have to get back with you on that. I'm not certain but based on the timeline, it is due this month. I'll get you some program information on that one.

Chairman Telemaco: Okay, great.

Robert Sellers: I just received it, as a matter of fact. It is done, it has been completed.

Chairman Telemaco: Even better, awesome. Thank you. I appreciate that excellent report.

Seeing no further questions, I'd like to move on to the next item. I'd like to recognize Sarah Harrell for the Identity and Access Management Update.

4. Identity & Access Management Update

Sarah Harrell: Good morning, Chairman and Committee members. For the record, I'm Sarah Harrell, Director of Enterprise Programs, and I'm here today to provide you an update on the Identity and Access Management Program, the IAM Program. My update will include a background overview and then a quick update on the active solicitation that will come back to this committee in Q4 for a recommended contract award. Next slide please.

To start with the background, what is Identity and Access Management? What is IAM? Gartner's definition is at the top of the slide in the blue outlined box. It's providing the right people the right access at the right time, plus being able to predict their access needs, and detect and respond to any inappropriate access that is detected. This goes to the heart of the earlier question of the Zero Trust. This program is about maturing the zero-trust mindset.

A little over a year and a half ago we engaged Gartner to do three things for us: to validate our internally developed Identity and Access Management Strategy, to do a Gap Analysis of our current state to the future state that is defined in the strategy, and then provide an implementation roadmap that would enable us to get to the future state.

There were five initiatives identified in that implementation roadmap and we'll see that in a couple of slides here. We began implementation in Q1 of 2020, and we're using a very standard implementation approach, multiple initiatives over a multi-year period.

Kelly Booten is the Program Sponsor; Robert Sellers is the Program Owner. He has, in fact, been the champion of this program from the outset. We have been providing intermittent updates to this committee, as well as to the Board since the implementation started. Next slide please.

A little more background is the "why" of the program, *why* are we doing Identity and Access Management? So, these are the business drivers, the business objectives, if you will. I'm not going to read the business objectives listed there, but the primary one, the first one listed and circled in red, is to reduce our cybersecurity risk. We need to mitigate the potential for a data breach or unauthorized access into our network as much as possible. We're never going to eliminate that risk totally, but the primary objective is to mitigate that risk as much as possible.

The next slide is the Implementation Roadmap with the five initiatives that I referenced earlier. Like I said, the implementation started in Q1 of 2020. The five initiatives are numbered essentially left to right there on the slide.

Two initiatives, Multifactor Authentication and Privileged Access Management, are operational with the gray "Operational" there.

The other two initiatives, three and four in the middle of the slide, are currently active, and that is the Identity Governance and Administration tool set and the Access Management tool set. Those two tool sets are active as a single solicitation, and I'll give an update on that on the next slide.

The fifth initiative in the yellow there is not yet active.

I know this is a lot of information, but I did provide a cheat sheet with a description of what these five initiatives are and what the intended business value from them are, and that's in the reference section of your materials.

My next and final slide is an update on the active solicitation that I referenced earlier. The Identity Governance and Administration tool set and the Access Management tool set is an active solicitation to procure those tool sets. The team is a little more than halfway through the evaluation phase. The cone of silence is in effect because we are in the evaluation phase, and there are 15 vendor responses in play. This solicitation is on track, as I referenced earlier, to come back to this committee in Q4 with a recommended contract award and then, of course, go to the December Board of Governors for approval.

There is a transparency note there at the bottom of the slide to let you know that the original ITN for the procurement of these two tool sets was cancelled and reissued as the current ITN. The cancellation and reissuance were to remove some unnecessary restrictive criteria in order to broaden competition. The reissuance was vetted and approved by Purchasing, Legal, and the Program Sponsors.

That concludes my updates. I'll be happy to take any questions.

Chairman Telemaco: Thank you, Sarah. Appreciate that report. Any questions from the Members?

Okay, seeing none, I would like to move on to the next item on the agenda and recognize Aditya Gavvala for the Enterprise Integration Platform as a Service Action Item.

5. Action Items

a. Enterprise Integration Platform as a Service (EIPaaS) Action Item

Aditya Gavvala: Good morning, Committee. This is Aditya Gavvala, Vice President - IT Services and Delivery. I would like to present the Enterprise Integration Platform as a Service Action Item to the Committee today. We are on tab 5A. There are two documents - an Executive Summary and the Action Item.

Let me start with the definition of what an Integration Platform, aka Integration Middleware, actually is. It is a piece of software that connects two disparate systems, moves data between systems while transforming the information on the fly.

The key benefits of an integration platform are data exchange, data mapping and transformation, governance, simplicity, and also the out of the box connections to modern technology platforms.

Citizens currently uses Oracle Fusion Middleware as an on-premises integration solution. There are over 350 integrations and over 200 file transfers built on top of this platform. The license model for this software is tied to the number of CPU cores. It also requires dedicated hardware. The dependency on physical infrastructure, lack of cloud compatibility, ever increasing license costs, and functional deficiencies make the product untenable for Citizens.

An enterprise class integration platform running in the cloud as a service would provide the key benefits of business agility, scalability, reduced cost, quick time to market, and rapid response to delivery.

An ITN was issued in January 2021 for soliciting an Enterprise Integration Platform as a Service. Twenty vendors responded to the ITN with five unique products. On August 18, 2021, a public award was made to select Oracle as the product, and AST as the implementation partner.

The Oracle product was not only highly capable and able to meet all of Citizens anticipated needs, it was the most economical choice offered to Citizens from the vendors that passed through to negotiations under the ITN.

AST, which is an implementation partner, is a world class systems integrator based in USA. They are an Oracle Cloud Premier Partner and authorized Oracle reseller. During the solicitation, the AST team demonstrated the most robust expertise in the Oracle Integration Cloud product. AST has several marquee customers using this particular product in both public and commercial sectors, including the City of Jacksonville, Florida and Orlando Airport Authority. AST is staffing the contract with a technical team that's highly qualified and experienced in migrating customers from the on-premises version of the product to the cloud version.

The Oracle product is expected to reduce costs, such as licenses, hardware, and utility software, approximately $2.6 million over the first five years. If Citizens renews this contract, the cost savings are expected to be even more significant in years 6-10. A detailed breakdown of the cost savings is shown on the next page.

In this table, the detail of the cost savings is broken down so, as you can clearly see, there is a five-year net cost reduction of $2.6 million. Typically, cost increases when migrating from on-prem versions of software to the cloud version, but this is a very unique case where we are

seeing a significant cost savings. That is due to the on-premises version of the products requiring dedicated hardware, and the license model is tied to hardware CPU cores. It also requires other third-party software products, so those are fundamental reasons why the cost of hosting it on-prem is higher than going to the cloud.

I'll pause for any questions at this time.

Governor Fields: Chairman Telemaco, this is Lazaro Fields. Can I ask a question?

Chairman Telemaco: Yes, please go ahead, Governor Fields.

Governor Fields: Aditya, thank you. I just have a quick question. I don't want to skip ahead too much, but in the next action item, there are approximately $9 million for software budgeted and $4.9 million for infrastructure as part of the Omnibus package. I assume, because the action item you're discussing now is separate, that the $3.9 million that you're seeking approval for now is not included as part of the later action item that's coming after, is that right?

Aditya Gavvala: Absolutely correct. The Omnibus only includes any contract renewals, extensions, anything that didn't have a separate action item. This being a separate action item it is not included in the next action item - that is an accurate statement.

Governor Fields: Okay, thank you.

Chairman Telemaco: Great question. Any other questions? Okay.

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

Chairman Telemaco: Yes, please go for the recommendation.

Aditya Gavvala: Staff proposes that the Information Systems Advisory Committee review and, if approved, recommend the Board of Governors:

a) Approve the contracts with Oracle America, Inc. and Applied Software Technology LLC for a base term of five years with optional renewal terms of an additional five years subject to future board approval, with an initial five-year contract amount not to exceed $3,996,287, as set forth in this Action Item; and
b) Authorize staff to take any appropriate or necessary action consistent with this Action Item.

Technical Advisor Brian Foley made a motion to approve the Enterprise Integration Platform as a Service Action Item and Governor Fields seconded the motion. Roll was called. The Action Item was unanimously approved.

Chairman Telemaco: Thank you, Aditya. We've got another Action Item to present. I'd like to recognize Kelly Booten for the Technology Infrastructure, Software, and Professional and Staff Augmentation Services Action Item.

b. Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part I

Kelly Booten: The Technology Infrastructure, Software, and Professional and Staff Augmentation Services - Part 1 Action Item is requesting contracting approval for a broad array of technology goods and services under the spend categories of Infrastructure, Software, and Professional and Staff Augmentation Services. This contracting approval is requested for purchases through the list of contracts specified in the Action Item, which includes certain existing Citizens-procured contracts, as well as certain State Term Contracts and Alternative Contract Sources approved by the State of Florida Department of Management Services. At the time of expenditure, Citizens staff will select the approved contract that provides the best value and meets the business needs of Citizens.

While this approach has been in place for quite some time, last year we started taking a two-part approach in an effort to provide further lead-time, transparency, and opportunity for review and questions by the Board. This current action item, Part I, is primarily focused on anticipated purchases in January through April of 2022[1]. A lot of the expenditures in the IT budget are front loaded towards the front part of the calendar year.

A second action item, Part II, will be primarily focused on anticipated purchases in May through December of 2022, and will be presented at the December ISAC and Board of Governors, and will correspond with the budget, as do these contracts.

The Action Item requests contracting approval in the amount of $17,232,557. The estimated contract spend is $4,955,926 for Infrastructure, $9,132,134 for Software, and $3,144,497 for Professional and Staff Augmentation Services.

The table on page two of the Executive Summary shows the breakdown from last year by each of these same three categories. Also on page two is a description explaining the approach and controls in place for proper oversight and accountability.

The action item further describes each contract, and details of each category and contract usage by category and contract.

The most notable change from '21 to '22 is the software category. The primary differences are due to multi-year contracts. There are two three-year contracts in last year's approval which total about $2 million that are not included in this year's; however, this year has three major three-year contracts up for renewal totaling $5,759,000, most notably the Microsoft License Agreement of $4.8 million. There is also an uplift of 4%, and there is a line-item detail that I can make available to any Board Committee member that desires it.

Part II will be presented at the December ISAC and is anticipated to be roughly $7.4 million. This is a very rough estimate. We've just started the budgeting process. We haven't made our final project selections that would be included in the budget that goes to the board, but we felt like this estimate needed to be provided for comparison purposes.

At this point, I will pause for questions before I read the recommendation.

Governor Fields: Chairman Telemaco, this is Laz. Can I ask a question?

Chairman Telemaco: Yes, please, go-ahead Governor Fields.

[1] Verbatim correction: Stated as 2020

Governor Fields: Kelly, so $17.2 million is the request, and this is only for January to April. Could you help me understand what the second part of this might look like in terms of a figure? Is it going to be another $17 million, or somewhere there abouts, or far less than that? And then the follow up question would be, I'm looking at the table on page two, could you just explain to me how this compares to prior years?

Kelly Booten: The $17,232,000 is for contracts that renew in the January to April timeframe. There are some multi-year contracts included in those expenditures, and I listed the higher dollar ones. The number for last year is listed on that table on page two. The estimate for Part II is $7.4 million. And this again, is a rough estimate because we're still working on our project selections for 2022, but it is less than the $11 million, if that number holds, for Part II of last year.

Does that answer your question?

Governor Fields: I think that makes sense. So, if I understand what you're saying, Part II for this year is forecasted to be approximately a little less than $4 million less than what it was last year on Part II. Is that right?

Kelly Booten: Correct.

Governor Fields: Okay. All right, thank you.

Chairman Telemaco: As a follow up to Governor Fields question, on the software expenses that have shot up for this particular Part I, I think you mentioned that it was due to multi-year contracts, $2 million of which, I think, was with Microsoft. Does that mean that it's coming off of a multi-year, so last year that expense wasn't there, and then this year it's multi-year so it's like two or three times what it normally would be?

Kelly Booten: Correct. To get pricing, some of the contracts are two or three one-year contracts. Microsoft is a three-year contract, so the last two years that hasn't been included in this action item. This year we're up for the three-year renewal, and it's $4.8 million.

Chairman Telemaco: Right. That would explain it.

Kelly Booten: Yeah, and it's hard to compare. We do our best to compare the prior year to this year, but there's so many ins and outs that you have to know, and projects change as well, and you can have a large project. So, for example, in this expenditure there are some services for Identity and Access Management. We anticipated having it fully loaded for this budget year but we won't be bringing this selection to the board until December so those costs will carry over into the next action item.

There is a lot of intricacy in this, but the reason we do it is because of the favorable pricing you can get off the State Term contracts. We do many quotes to get that pricing; we don't have to bring it back every board meeting for each of the individuals underneath it. We did take a stab at the anticipated expenses for each of the contracts listed, which is hard, as well, because you don't know which one's going to turn out to be the best one at that point in time. We did put those numbers together, and again, it's the Microsoft contract that's the highest. The GSA Schedule 70, we use that one quite a bit, as well.

Chairman Telemaco: Excellent. What's clear to me is that all of these expenses and all of these contracts are all already vetted through the internal purchasing department, vendor management process. The items themselves would have previously been approved; this is just changes, modifications, extensions. This isn't like a slush fund of money that's just being pre-approved for spending; it's all already been earmarked. Is that correct?

Kelly Booten: It's absolutely monitored and tracked in detail, and nothing can be purchased that hasn't gone to the Board for pre-approval, if it's over $100,000. We actually include all expenditures in this, and also, we ask the question if it's budgeted or not.

Chairman Telemaco: Right. Thank you for that clarification.

Kelly Booten: May I read the recommendation?

Chairman Telemaco: Yes, any questions before we ask for the recommendations? Any further questions? Okay, seeing none go ahead, Kelly, and read the recommendation.

Kelly Booten: Staff recommends that the Information Systems Advisory Committee recommend to the Board:

a) Approval of the Technology Infrastructure, Software, and Professional and Staff Augmentation Services Part 1 contract for an amount not to exceed $17,232,557, as set forth in this Action Item; and
b) Authorize staff to take any appropriate or necessary action consistent with his Action Item.

Governor Fields made a motion to approve the Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part I Action Item and Technical Advisor Brian Foley seconded the motion. Roll was called. The Action Item was unanimously approved.

6. New Business

Our next and final item is New Business. Is there anything new that any member would like to raise before we adjourn this meeting? Seeing none, our next ISAC webinar is scheduled for December 7 at 10:00am, and I look forward to seeing some of you at the next Board meeting in a couple of weeks.

Thank you very much for the excellent reports this morning. If there are no other comments or questions, I'd like to thank you all for your time and I will entertain a motion to adjourn the meeting.

Governor Fields: Move to adjourn.

Chairman Telemaco: Thank you. Enjoy the rest of your week and see you all in a couple of weeks.

(Whereupon the meeting was adjourned.)