Information Systems Advisory Committee March 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 August 30, 2022
Purpose/Scope	Review of the August 30, 2022 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 August 30, 2022 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
Tuesday, August 30, 2022

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened via Zoom webinar on Tuesday, August 30, 2022, at 10:00 a.m. (ET).

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

Jason Butts, Chair
Erin Knight
Nelson Telemaco
Brian Foley
John Vaughan
Kelly Booten, staff

The following Citizens staff members were present:

Aditya Gavvala
Barbara Walker
Bonnie Gilliland
Chris Jobczynski
David Woodruff
Eric Addison
Ray Norris
Robert Sellers
Sandy Allison
Sarah Harrell
Stephen Guth
Wendy Emanuelson
Wendy Perry

Roll was called and a quorum was present.

1. Approval of Prior Meeting's Minutes

Chairman Butts: Good morning, everyone. Thank you for joining the meeting today. I would like to call this meeting to order and seek approval for the prior Minutes. Do I have a motion?

Governor Nelson Telemaco made a motion to approve the August 30, 2022, Information Systems Advisory Committee (ISAC) Minutes. Governor Erin Knight seconded the motion. The minutes were unanimously approved.

Chairman Butts: Thank you very much. I would like to turn it over to Kelly Booten, the COO, for her update. Kelly.

2. Chief Operating Office Update

Kelly Booten: Good morning, Kelly Booten for the record. I'm going to cover today the ISAC dashboard which is in section two.

The upper left quadrant of the dashboard is the IT Finance section, and the budget to actuals are on track through second quarter of 2022 at or around 50 percent or below of the targeted 2022 budget. We are below 50 percent in some cases due to cost savings or delays in projects.

The upper right quadrant is the Top Technology Strategies & Alignment to Themes. There are five strategies I would like to briefly highlight today.

For Cloud Migration, the procurement phrase was marked complete since the last committee meeting as the contracts for the cloud platform are covered by existing contracts or will be covered through the annual budgeting and contracting provision. This project is slowly moving forward filling in around other higher priority initiatives. On average we migrate one to two applications per month.

For the Applications Integrations Platform item, the procurement was previously completed and is now showing a gray color for on hold. However, as reported at the last meeting, this project was suspended due to issues with the vendor, so we are continuing to look at alternatives. We have this currently budgeted using the current software for 2022, and we intend to have a long-term plan ready to bring forward in December.

For the Analytics and Data Warehouse Modernization, we are in the negotiation phase. Negotiations are being held as we speak. We had 18 vendors that submitted proposals with nine vendors moving forward to negotiations. Our plan is to also bring that one to the November/December Board meeting.

For Unified Communications, the procurement is also currently in the negotiation phase. The evaluation team identified eight products for the CCaaS and eight for the UCaaS as potential solutions, so we had multiple vendors offering these products. They were also advanced to negotiations. With this number of vendors moving forward the negotiation team needed additional time. The award is actually today, and the solicitation will now be presented at the November ISAC and December Board meetings.

For Citizens' Eligibility Reimagined, this ITN is also in the negotiation phase with two vendors developing proofs of concept. The POC demonstrations were held last week for each vendor, and we do have additional discussions with the vendors as we move forward through the negotiation phase. No doubt this is a very complicated engagement as we try to ensure that the solution meets our business objectives. This one will go to the Exposure Reduction Committee at the December Board meeting.

The last three solicitations mentioned are in the cone of silence.

In the lower right quadrant is the Risk and Security section. There are no high risks consistent with the last report. At the last meeting we had five medium risks and five low risks. They are now ranked at six medium and four low, and this is because we combined about nine items underneath the Life Cycle Management category, and elevated that one to a medium risk. We are working through those risks as we always do. This one is a moving target, it changes constantly. And there was no change in the top five categories.

On the lower left quadrant is the Resiliency side. All 2022 catastrophe readiness tasks have been completed successfully. Catastrophe performance testing was also completed successfully. We had a few findings that we're working as performance enhancements, but by all measure we've made it through that test. The overall state of Resiliency Readiness and the PIF Scenario

Planning Assessments are also 100 percent. Robert's going to cover these two later in the agenda.

So, with that, I will pause for any questions.

Chairman Butts: Seeing none. I would like to go ahead and turn it over to Robert Sellers for the IT Security, Risk, and Resiliency Update. Robert.

3. IT Security, Risk, & Resiliency Update

Robert Sellers: Good morning, Governors and Advisers. Robert Sellars, CTO for Citizens Property Insurance. This morning we are going to cover, as we do each year at this time, the status of the IT Security Program and our Enterprise Resiliency Programs. Wendy Emanuelson, the Director of IT Security & Risk is going to take you through the IT security component. Wendy has been in her position with Citizens since December of last year and has been with Citizens about three years now.

As you understand in your own business and in our world today, the business of IT security and risk is a never-ending set of activities. We have constant threat actors around the world attempting to impact organizations through criminal activities, through general tendency to want to find information and use it inappropriately in our world of automation and technology that we have today that we are all so dependent on. It is a program that we continue to invest in. We continue to spend time analyzing the different threats, analyzing the prioritization on treating those threats, and making appropriate investments to do so.

Wendy, as I indicated, is going to take you through. At this point I would like to introduce her and have her take over the presentation.

Wendy Emanuelson: Good morning, thank you. Today I will present our updates to the IT Security & Risk Program for this year. I'll highlight changes from the program that was updated and presented last year. Next slide, please.

The IT Security & Risk Program aligns with the Enterprise Risk Management Framework which incorporates a widely accepted three lines model approach to governance and risks. You have likely seen this slide before, so I'll just highlight some of the main areas that make up the three lines model.

As identified here the three lines model identifies the first line of our business as our business in IT operations management who own the security controls and risks. This is where the divisional risk tolerance is established and where operational and departmental policies and procedures are developed that guide operational activities, as well as risk identification, evaluation, and management.

Enterprise Risk, the Risk Steering Committee, the Privacy Office and IT Security & Risk all function at the second level. Here governance, guidance, risk management, controls, enterprise policies and standards are at the core of the second line.

Finally, at the third line the Office of Internal Audit provides independent and objective assurance. They validate the effectiveness of the operational controls and the overall risk of management framework while keeping the executive leadership team and the Board of Governors informed.

The ELT and Board make educated IT and security risk management decisions within Citizens' risk tolerance levels. The three lines model emphasizes the key principles of communication, cooperation, and collaboration to contribute to protection and creation of value within Citizens. Next slide, please.

This next slide gives you a graphical representation of the frameworks that are at the core of the IT Security & Risk framework. As mentioned previously, IT Security & Risk have adopted a collaborated mindset to align and partner with Enterprise Risk; therefore, the frameworks they align to become the foundation at our core. IT Security & Risk has developed a hybrid approach to risk management as well as governance. Employing our IT security control set made up of the essential 18 critical security controls published by the Center for Internet Security and lining them with NIST cyber security and privacy frameworks to deploy controls that perform what the National Institution of Standards and Technology has identified as key to cyber security and privacy, those being identify, protect, detect, respond, and recover. Next slide, please.

Now that I have briefly outlined what industry standards and frameworks lie at the foundation of our IT Security & Risk Program, I'd like to now take the opportunity to describe how Citizens' IT Security & Risk team applies these to help Citizens operate securely. The remaining slides of this updated presentation contain more changes from last year's update, which represents how our team has evolved to adjust to the ever-changing threat landscape, technological infrastructure, and the agile environment for which Citizens operates. The IT Security & Risk team has defined the following as its mission: 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. Next slide, please.

The IT Security & Risk team has defined five guiding principles that help us deliver value to Citizens as we carry out our mission. We protect confidentiality, integrity, and availability by delivering controls progressively to mitigate risk and protect data. We enable risk- based decisions by providing transparency around cyber security risk to aid in decision-making. We partner with stakeholders to address risks, promote accountability, and risk ownership. We present options for risk treatment mitigations that support organizational priorities, and then invest and provide guidance to manage risk through alignment of investments and resources with organizational needs.

One might ask us how and when to apply which principle. Our mission requires that each one of us deploy these principles with every engagement where appropriate, but we are always thinking about how risk and security can be impacted. Making sure that we are partnering with the business and IT and presenting them with the facts and options to enable them to address risks within their solutions, we help protect Citizens. These principles are key to keeping Citizens' operating environment safe, secure, and resilient. Next slide, please.

These guiding principles have been at the forefront of my team's goal since my appointment as Director of IT Security & Risk. Through seeking to deploy these principles we've seen an increase in security engagements. On this slide you'll see our highlighted accomplishments from 2019 through year-to-date. I won't include all of them, but I do want to highlight some.

- Above 98 percent usage of multi-factor authentication for remote system access.
- We also reduced local administrator usage by greater than 80 percent, reducing the risk of malware spread.

- We facilitated closure of over 80 percent of exceptions to policy, 97 percent of open risk gaps related to standard security controls, as well as closure of 16+ audit projects with open items.
- We've consulted on over 200 engagements throughout the organization. That includes 75+ security reviews which include IT, security standard assessments, security contract language reviews, and vendor security on organizational control reports.
- Our phishing campaigns have resulted in a 100 percent increase in phishing reports, and during the last quarter only 8.25 percent of our staff were identified as phish prone. On average, Citizens receives 150 actual phishing attempts per month, and only two to three user clicks.

While these are not the only accomplishments over the last three years, these do highlight some of the areas where reduction of risks can make a big impact in countering today's threat landscape. Next slide, please.

Additionally, there have been some notable improvements and accomplishments over the last year regarding our Enterprise Data Incident Response Plan or the EDIRP. In partnership with Legal and Privacy, we've educated and exercised the plan. We've enhanced the process for response to third-party incidents, and we've internally reviewed our capabilities to respond rapidly to a major incident, including our managed services. Finally, we've updated our run books and quick reference guides. Next slide.

Last year, the IT Security & Risk program had six strategic objectives. Those are identified on the left of this slide. We have transformed and combined the *Advanced incident, threat and vulnerability detection, protection and response practices* with *Optimizing Citizens' cloud security platform and architecture*. We have combined those into one strategic objective, *Optimize IT Security Operations and Architecture Capabilities*. Citizens' migration to a cloud has influenced this holistic optimization of the overall IT security and operations and architecture capabilities. Next slide, please.

This slide is IT Security & Risk Strategy on a Page and was presented last year; however, it has received some minor updates, most of which have previously been discussed already. I won't spend too much time on this slide, but I do want to point out the risks and assumptions that are key items not previously discussed in this presentation.

Risk to our strategy execution can include legacy systems and security technology infrastructure. This is a risk not unique to Citizens; however, nonetheless impactful. We must ensure we are staying vigilant to ensure legacy systems are secured and monitored while those dependencies still exist, as well as managing the retirement of these systems in a timely manner.

Next, achieving thorough visibility into supply chain partners. Security and compliance posture may be challenging. Advancing our third-party risk management capabilities will help to mitigate this risk. IT Security & Risk has been collaborating and partnering with Vendor Management and Purchasing to help advance in this area. For example, contract reviews, security organization certification reviews and questionnaire response evaluations.

Unexpected changes in the regulatory threat landscape are another risk. The pandemic and the move to the predominantly remote workforce is a prime example of this. While Citizens stepped up to this change quickly and successfully, the unexpected will always remain a risk.

Next, the integration of security and motoring tools with SaaS-based applications, Software as a Service. This may not be possible. ITSR engagement is important when making decisions on adoption of SaaS-based solutions. We participate in the governance process to ensure we're providing risk-based information to those making decisions on the solution of choice.

Finally, the assumptions: ITSR foundation includes the program support of leadership, so leadership support is at our foundation; IT support for implementation, integration, and operation of security platforms; a clear understanding that activity that rises to enterprise level will managed through enterprise level governance processes; and lastly, that the security technology staff may need to be expanded to fulfill the program.

Appendix A, the next slide, has been provided for your convenience with definitions of terms used throughout the presentation. Appendix B has provided, been provided to you as additional information.

Thank you for your time today in allowing me to present IT Security & Risk Program updates. I am happy to answer any other questions you may have at this time.

Chairman Butts: Wendy, thank you very much for the update. I just have one question on the slide before, I believe on the executive summary page. The ongoing threats and looking ahead, one of the notes on the security culture, how can we increase that employee engagement in security awareness completing the phishing videos and other training materials that maybe your team puts out?

Wendy Emanuelson: One of the things that we're looking at is, besides the phishing campaigns, also gamifying some of the training as well. Making it up front and present more often. So, monthly articles, quarterly newsletters, reminders in a timely manner, such as during holiday seasons, travel seasons, things like that, always identifying what could possibly be out there, and keeping the communication lines open. We've seen a great change in the culture. Instead of us pushing, we are getting a lot of pull in, which is awesome. We will continue to do these things and seek out every opportunity we can to assist and advise.

Chairman Butts: Perfect, thank you. Any other questions? Great, thanks, Wendy.

Wendy Emanuelson: Thank you.

Chairman Butts: I will turn it back over to Kelly Booten for the Technology Infrastructure, Software, and Professional and Staff Augmentation.

Robert Sellers: Excuse me, Governor Butts. I'm going to continue with an Enterprise Resiliency update as well.

Chairman Butts: All right, perfect.

Robert Sellers: Thank you. I do want to mention one other thing that Wendy's team has recently undergone in the area of gamification of security events and security training. Many of us have heard of the escape room experience where you travel and spend time with a group of your friends, finding a way to get out of the room. Recently her team underwent a training exercise very similar to that, only done virtually and focused around escaping from a security event and dealing with that, all the challenges associated with that over a virtual environment.

The team did manage to escape after an hour of their time, as well as handling a number of additional questions and challenges that were brought forth by the vendor. This is an area that we do have to make fun. It's a serious business, no doubt about it, and it is becoming part of our lives in everything we do daily with our own personal, financial, and other private information, but even more so with the information that we're entrusted to as an organization. I look forward to continuing to see this type of pull and push activity through our training, through our newsletters, through our engagement with our organization.

Continuing forward with the Enterprise Resiliency Program, Enterprise Resiliency is around the process of providing a methodology to anticipate and respond to events. Typically, unexpected events, some we can plan for, but many times they come from unexpected directions and bring the organization back into operational status.

We start with the business impact analysis where we go through all the requirements that the organization has for resiliency, looking at our people, process, and technology, analyzing what is our risk tolerance in these areas of resiliency, and then identifying the strategies and implementing those strategies and risk mitigations.

The operational resiliency is the initiatives that expand our business continuity business programs, looking at all these different risk issues and ensuring that our employees, our customers, our citizens, and our partners have the ability to continue in their daily activities associated with Citizens' business. Let's go to the next slide, please.

This is a graphical overview of the program entities that I am going to talk about this morning. When you look at our resiliency program, it is very broad in scope. It covers ground in our crisis area, as well as our technology areas, as well as our ability to respond to storm catastrophe activity. This information and this particular team led by Sandra Allison, our manager of Enterprise Resiliency, developed with the business these resiliency plans. You'll see as we go further through that we have 18 different plans associated with this that makes up our Enterprise Business Continuity Plan. That plan is utilized by a number of different organizations as part of their due diligence into our ability to respond to different types of events, whether it's our reinsurance vendors who want to have confirmation that we are able to handle claims or our other processes appropriately, or by the Office of Insurance Regulation as part of their Market Conduct studies. We are being looked at constantly in these areas; do we have the ability to respond, are we resilient as an organization? Let's go ahead to the next slide, please.

To do this, we have a significant amount of governance and organizational alignment. This committee here, as well as our Enterprise Risk Management organization led by Joe Martins, work to help provide guidance and direction to the organization. The Enterprise Resiliency Committee that is made up of our senior leadership inside Citizens, and our IT Governance and IT Risk Management Committees that are made up of our senior IT staff work to ensure alignment.

We have a number of updates throughout this last period, 2022-2023, focused on our operational resiliency down through our IT systems recovery which is known as disaster recovery, and our resiliency planning and exercises. Let's go ahead to the next slide, please.

The Operational Resiliency Program was initiated last year. This was a focused look at our organization to ensure that with the increasing PIF counts, now at over a million in terms of our policies in force, and looking at the growth scenarios, as well as the potential for what we would do as the policies in force shrunk, we went through with over 48 different teams across the organization looking at the people, our processes, our technology, and our third-party vendors to determine where impacts would take place as the policies continued to grow.

Results of this impact analysis: We work to increase our staff and adjust the scheduling, all the way through technology, optimization activities, improve monitoring to ensure that we knew up to the minute how these systems were performing. A number of different resiliency activities are in place now that have already been completed and are continuing to move forward as we examine the continued growth. We meet on a regular basis with the business and with other parts of our technology organization to maintain focus on our operational state for this increased growth. Let's go ahead to the next slide, please.

So again, the PIF areas that we are looking at in the technology area, which is the start of the cycle, are our applications, whether it is the underwriting processes or the claims or the financial areas. Our capacity on the basic technology, our protection and resiliency of these systems, how well our networks are running, how loaded they are, and then of course, all the operational work that goes into running the business on these platforms. Everything from printing of underwriting and claims to securing the systems for increased workloads. Go ahead to the next slide, please.

Our business continuity plans, I mentioned 18 different plans that formulate the entire plan. You can see here the different areas of the organization that have continuity plans formalized and reviewed on a regular basis. We have maintenance cycles where we go through with the resiliency coordinators from each of these groups, reviewing their practices, anything new that had been added, ensuring that they have the appropriate broad view into what it takes to continue that operation. Not just by themselves with their particular area, but also at the enterprise level as well as the group. Let's go to the next slide, please.

As part of that we also have a validation program. Again, during the early part of the year, we had a number of different exercises, completing and finishing most of those up by August. We have a few more to accomplish here in the September and November time frames for these to be completed. And note that the focus on all these exercises, we have different types of scenarios. One this year was the mission critical system outage. In alignment with that, also a ransomware exercise. What happens to these business continuity plans when the systems are not available for differing reasons? Let's go ahead to the next slide, please.

We have a wide variety of systems in our organization, some considered mission critical, others going down to business critical, and further down in the scale. You can see here on this particular slide; we have some very small windows of operational time frame to bring these systems back to make them available for the business users before they have to go into their continuity plan of operations. So, when you look at our claims systems, within eight hours these systems have to be up, operational, and available in order for the teams to continue their processing; going down to up to two weeks for other systems. Let's go ahead to the next slide, please.

In the area of Resiliency and Disaster Recovery Posture, Kelly started the briefing this morning with the lower left-hand corner having our current state of resiliency. One of those areas was the IT and Disaster Recovery process. We look at the functional areas and our ability to recover those systems if we were to have a technology failure, our resiliency on cloud technologies, as well as our on-prem technologies, different testing activities. We are constantly evaluating our ability to fail a system to a secondary device or to a secondary system. Systems are built with resiliency in mind. Our data centers have been built with resiliency in mind, and our cloud infrastructure has been developed with resiliency and disaster recovery in mind, as well, all key priorities for the organization. As you can see down at the bottom of the slide, our readiness is, at this point, all green. Let's go ahead to the next slide, please.

Our CAT Assurance is another one of the pillars of the Resiliency Program. Again, as Kelly mentioned, we had over 140 checklist items this year. We are complete in that activity, and that includes actually running the systems through our test processes at the volume loads anticipated for 2022 with a 350,000-claim event. We will continue to increase that as our policies in force increase and continue to test that. We are now testing in the organizational resiliency program for a number far beyond the one million policies in force and the 350,000 claim events.

Our field readiness vehicles that are prepared, trailers, satellites, other types of communications, are available to roll to different parts of the state. In our areas for remote work, many of our staff are already working remotely, independent adjusters clearly work remote, and we have everything exercised and ready to go for, hopefully, no storms in 2022. Let's go ahead to the next slide.

Again, I follow up with the image here giving you again the pillars of our Resiliency Program. It is a very large program covering the entire organization, and while we have a small staff with Sandy Allison and two additional resources to organize and structure the program, this really is very similar to our IT Security & Risk program and enterprise-wide program. It has to be a pull and is engaged with many different members of our organization working to ensure the resiliency of Citizens if we were to have any type of unexpected event.

With that, Governors, I will take any questions that you might have, and I just want to thank you.

Chairman Butts: That's a great update and I appreciate that. Any, any questions?

Governor Telemaco: Yes, good morning. Great, great presentation, thank you for the update. My question is, as technology evolves, as the world evolves, we are all heading into web 3.0. I'm curious if you have identified any areas of development, focused development for our team? You guys have done a great job to this point, but is there any way that we can support you and your team to be ready, from a competency point of view, with what we're likely to see in the coming years? I just wanted to ask that question as an open question and ensure that you know that all of our intentions are to support the team to continue to do the great work you are doing.

Chairman Butts: No one? Anything?

Kelly Booten: I'd say support the budget, of course, as we bring items forward for the training needs that the staff has requested and management has thought is important in this area. We'll take a hard look at that and make sure that we've got everything accounted for when we bring our budget forward. And I see Sandy jumping on, so maybe you have something you wanted to say.

Sandy Allison: No, that is exactly what I would have said, Kelly. That's why we are so successful today is because we've had that support throughout from the executive team, and as long as we continue to get that support, we'll be good.

Governor Telemaco: Great, awesome. Thank you.

Chairman Butts: Thank you, Governor Telemaco.

Brian Foley: Robert, this is Brian. As the world moves more towards true high availability and hot, hot capabilities for your most critical applications, I'm assuming you are looking at what those are and what needs to be done so if there is an automatic failover for those kind of things as opposed to recovery is more of high availability. Does that make sense?

Robert Sellers: It truly does. The design for resiliency, as you indicated, the always on model. We are so familiar with that in our own personal lives. Our ability to get on our phones and be able to connect to our bank account and to see a balance. The moment that phone doesn't connect, up pops a message that says, sorry, we are in a maintenance mode, or even worse, you are not getting any response as to why. The always on model of technology is pretty much here today. The expectation by the consumer used to be dial tone. You used to be able to pick up a phone and you always had a dial tone. Well, today in our world it is, you connect to a computer, you expect to be able to do the action that you are attempting to accomplish, right then, right now.

We are starting with that at fundamental and foundational levels. Our database work, we've been doing that for several years now with the always on model, replicating and keeping data current and the ability for the technology to switch between the environments seamlessly, as needed. The cloud technologies that we are implementing, we are also putting into place that resiliency and those automated, always on types of technology, running in different areas of the country, running in different multiple networks so that there isn't a loss of availability and there is immediate fail over if there is an event and the system stays available to the user.

So, Brian, to your point, that is an area that has to be designed into the platforms that we are acquiring. It has to be designed in, many cases, for the software that we are acquiring, as well. As we go through our technology road maps, that is becoming and is a principle of our architectural foundations to ensure that the capabilities of the software and the hardware is there to meet the needs of the organization through that type of resiliency that you are speaking to.

Brian Foley: Yes, and it also changes the way you develop software, not just acquiring software. Developing software needs to be able to take advantage of the components you've put in place from an infrastructure perspective to fail over.

Robert Sellers: That is correct. Both the software that we develop in-house using what I would call our lower code level type designs and our low code designs, as well as the software we acquire from our vendors. We do a significant amount of work with third parties' software, constant solicitation as we get into the life of software, and those are areas that not only do we have to design for and build into our software catalog, but we also have to ensure we acquire appropriately for that, as well, during the solicitation phases. It is a constant cycle. I talked about security and constantly looking at the threat factors for the organization, we're also doing the same with our software. It is an important part as you mentioned, Brian.

Aditya Gavvala: Brian, this is Aditya. I just wanted to reiterate what Robert said. Our foundational principle for infrastructure, architecture, and application architecture is leveraging automatic fail over and high availability that's provided by the underlying platform. It applies not only to the infrastructure component, as you rightly pointed out, it applies to any bespoke applications that we develop or any enhancements that we do to Software as a Service products or the commercial off the shelf products.

Chairman Butts: Thank you. Any other discussion or questions? Perfect. Thank you very much. Kelly, back over to you I believe.

4. Action Item

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

Kelly Booten: Good morning again. I am going to use the Executive Summary as the basis for the explanation of the Technology Infrastructure, Software, and Professional and Staff Augmentation Services - Part I Action Item.

This is the annual request for contracting approval of 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 existing Citizens' procured contracts, as well as certain state term contracts and alternative contracts sources that are approved by the State of Florida, Department of Management Services. This action item, which is called Part I, is primarily focused on anticipated purchases in January through April of 2023. The second action item, Part II, will be primarily focused on anticipated purchases in the May through December 2023 time frame, and will be presented at the December Board of Governor's meetings along with the budget. All these items will be included in the 2023 budget, also presented in December, and then multi-year items will be included in subsequent budget years.

This action item requests contracting approval in the amount of $18,935,361 under those three spend categories. The estimated contract spend is $6,684,344 for infrastructure. $5,995,410 for software, and $6,255,607 for Professional and Staff Augmentation Services. The projected contract spend by category is summarized by section within the action item executive summary starting at the bottom of page 1.

The first paragraph on page two includes the infrastructure major expenditures. For example, there is an item, $2,781,938 for telecommunication needs, and that includes everything related to telecom. There is an item for $1,437,360 for data center and field service vehicle storage and rental, that data center contract is the three-year term; and then $1,186,959 for hardware service and maintenance needs.

At the bottom of page 2 is the anticipated major expenditures for software: $3,128,273 for enterprise applications such as Java support, video platform, application, and server database software; $1,984,626 for the data center software which includes network support and maintenance, user data backups, and log analysis tools.

At the bottom of page 3 are estimates of projected material expenditures for Professional and Staff Augmentation Services: $4,290,479 for Staff Augmentation Services. The predominant category underneath that is application development, but it also includes security resources, big data analytics, tier II operation support. There's an item for $1,202,000 which is for enterprise applications such as our ERP system, Microsoft professional services, and application development. And then there's a $518,232 item for information security professional services.

At the top of page 5 is a table that denotes the total anticipated spend and a breakdown of the three spend categories for 2022 Part I and Part II, and 2023 Part I, which is what we are asking for approval today.

It's difficult to get an exact apples-to-apples comparison of each part due to the contract expirations and changes in projects year over year, but we can generally explain significant ins and outs. The 2023 Part I compared to 2022 is overall $1,702,804 higher. This includes an annual increase assumption of four percent over the prior year for most of the line items.

In the Infrastructure category it is higher by about $1.7 million, predominantly driven by the addition of the data center three-year renewal of 1.3 million, which I previously mentioned, and the expenditures for new field service vehicle equipment.

The software category is $3,138,724 lower than last year due to this year not needing to include the Microsoft licensing which was a three-year term. It was a significant expenditure last year and there were a couple of other large software renewals that are not included this year.

For professional staff augmentation, it's $3,111,110 higher due to project needs to compensate for staff vacancies and increase demand in operational, as well as business need. Here we use staff augmentation to help us compensate for backlogs in staffing, retention when we have turnover. If we keep our staff at 100 percent, then we don't need as much spend in this category.

We do have a line-item detail that I can provide to any committee member if you want it. And if there are no questions, I can read the recommendation.

Chairman Butts: Any questions for Ms. Booten? Perfect, Kelly. Go ahead and read the action item, please.

Kelly Booten: 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 in an amount not to exceed $18,935,361 as set forth in this action item, and authorize staff to take any appropriate or necessary action consistent with this action item.

Chairman Butts: Do I have a motion to accept as read?

Brian Foley made a motion to accept the Technology Infrastructure, Software, and Professional and Staff Augmentation Services – Part I Action Item. Governor Nelson Telemaco seconded the motion. The Action Item was unanimously approved.

5. New Business

Chairman Butts: Is there any new business or any additional questions? Seeing none, I would like to thank you again for joining us today. The next ISAC meeting is scheduled for November 29th and look forward to seeing many of you at the Board meeting next month. I hope everybody has a great day and the meeting is adjourned.

Kelly Booten: Thank you.

Chairman Butts: Thank you, have a great day.

(Whereupon the meeting was adjourned.)