# ACTION ITEM



**Information Systems Advisory Committee Meeting, December 8, 2020**
Board of Governors Meeting, December 15, 2020

| | |
|---|---|
| ☐**Contract – New** | ☒**Committee or Board Minutes** |
| ☐**Contract – Amendment of Contract Terms** | ☐**Product Changes** |
| ☐**Contract – Additional Spend** | ☐**Other _____** |

| | |
|---|---|
| **Contract ID** | Information Systems Advisory Committee Meeting Minutes<br>September 8, 2020 |
| **Budgeted Item** | ☐Yes<br>☒No – N/A |
| **Procurement Method** | N/A |
| **Contract Amount** | N/A |
| **Contract Term(s)** | N/A |
| **Purpose/Scope** | Review of the September 8, 2020 Information Systems Advisory Committee Meeting Minutes to provide opportunity for corrections and historical accuracy. |
| **Recommendation** | Staff recommends the review and approval of the September 8, 2020 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, September 8, 2020**

The Information Systems Advisory Committee (ISAC) of Citizens Property Insurance Corporation (Citizens) convened via Zoom webinar on Tuesday, September 8, 2020 at 11:00 a.m. (ET).

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

James Holton, Chair
William Kastroll
Brian Foley
John Vaughan
Kelly Booten, staff

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

| | | |
|---|---|---|
| Aditya Gavvala | Chelsea Garfield | Ray Norris |
| Barbara Walker | Dan Sumner | Robert Sellers |
| Barry Gilway | David Woodruff | Sarah Harrell |
| Bonnie Gilliland | Eric Addison | Stephen Guth |
| Carlos Rodriguez | Jennifer Dilmore | Wendy Perry |

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

**1. Approval of Prior Meeting's Minutes**

**Chairman Holton:** Welcome everyone to the September ISAC teleconference. The first order of business is approval of the prior Minutes. Are there any corrections? None being heard, I will accept a motion to approve.

**John Vaughan made a motion to approve the June 1, 2020, Information Systems Advisory Committee (ISAC) Minutes. Brian Foley seconded the motion. Roll was called. The minutes were unanimously approved.**

**Chairman Holton:** Next on the agenda is item two and the Chair recognizes Kelly Booten for her report.

**2. Chief Operating Officer Update**

**Ms. Booten:** Good morning. For the record, Kelly Booten, Chief Operating Officer. Today I would like to provide a status of IT and vendor-related audits, and an update on the IT GROW Program.

The Office of Internal Audit will report to the Audit Committee on five audits and advisories with IT or vendor-related components that were completed since the last Board meeting.

One is the Service Organization Controls (SOC) Audit. Citizens requires prospective and current vendors to provide a Service Organization Controls Report when services that are procured are either cloud-based with access to Citizens' confidential or restricted confidential data or services that are procured that could have a potential impact to Citizens' internal controls over financial statement reporting. The audit identified the need to implement a SOC control exception tracking and monitoring process to ensure the vendor remediation plans have been completed to resolve exceptions, if identified. The process to remediate this one finding is anticipated to be closed by the end of October.

Second is the Third-Party Access Audit. The objective of this audit was to evaluate risks associated with third-party access to Citizens' information resources and validate that third-party access policies, inventories, user access management, connections and monitoring are appropriate for the organization in mitigating these risks. Internal audit noted policy and process improvements since their last audit of third-party access. The Information Technology Security Policy, Information Technology Security Standards, the Vendor Management Office contract template and the Vendor and Contract Management Playbook have been updated to include specific provisions concerning third-party access since the last audit. IA also noted that a Third-Party IT Security Governance and Access Matrix had been developed to delineate program responsibilities. Their work indicated two areas where operational controls could be strengthened to ensure that third-party access to Citizens' information resources is properly managed. Both items are anticipated to be closed by the end of the year.

Third, OIA provided control advice and project support services for the Agency Management System implementation. In July, the new Agency Management System, myAgency, was implemented. The system provides agency principals and agency principal designees the tools to manage all their Citizens-related administrative needs in one system. Citizens will use myAgency to more effectively collect, maintain and make more readily accessible information about the size and quality of each agency's relationship with Citizens. It was designed, developed, and implemented on the Salesforce platform by a team of Citizens' employees within the Enterprise Operations Division. I would like to recognize Aditya Gavvala and Carl Rockman for their leadership in getting this implemented. With this engagement, OIA provided advice and guidance, relative to Phase I of the project to implement the myAgency platform. IA provided consultative support over areas of elevated risk to the implementation to provide assurance of the design and control of the activities. It was a very successful implementation.

Next, OIA also participated in and provided advisory services for the Citizens Insurance Suite Disaster Recovery Test. IA was asked to participate in the DR exercise and provide feedback regarding the attainment of plan objectives, the validity of management's observations from the exercise, and a list of strengths and opportunities based upon the results. Following the conclusion of the exercise, IA reviewed the exercise results and agreed with Management's conclusion that the exercise met the failover plan objectives. Several strengths and one opportunity were noted by IA: operational procedures were executed in less time than is required by the business impact analysis; user testing was completed; reporting and change management process were followed; there was one application that recently migrated to the cloud that required remediation.

Last, as part of the Centerpoint User Access for Financial and Procurement Role Redesign Implementation, OIA tested role configurations and provided advice on the adequacy of access provided. There were four roles identified as being potentially over-privileged, for which Citizens engaged Ernst & Young to provide remediation recommendations. All four roles were remediated, tested, and set up into production.

Also, today I would like to report on our IT GROW Program. One of IT's recruitment strategies we call the Grow Program has officially come to fruition. It had a little bit of a bump in the road due to COVID, but we did successfully launch and have partnered with Florida State College at Jacksonville, FSCJ, to prepare students for jobs in Application Development and in IT Security & Risk. Through a 98-hour program, students will earn industry standard credentials, and some may land paid internships or jobs at Citizens.

The tailored curriculum of this specialized program is designed to meet the unique requirements of Citizens and the insurance industry, and was developed partly in response to the ongoing difficulty in staffing hard-to-fill IT positions.

This training program between Citizens and FSCJ consists of four-course curriculum: Information Security, Software Development, Microsoft Azure Fundamentals, and Agile Fundamentals.

As of Friday, we have 12 students enrolled of which six are employees. The kickoff for the class starts tonight where Robert and Aditya will be talking to the students.

For today's agenda - the next three agenda items are updates on topics that are included in the ISAC Charter and the IT Strategic Plan - the yearly Enterprise Resiliency and IT Security & Risk Updates - and an Identity and Access Management Program update.

That concludes my report. I can entertain any questions or conclude the report.

**Chairman Holton:** Thank you, Kelly. Members, any questions for Kelly? Okay, thank you again, Kelly, for that report.

We will now turn to agenda item three and the Chair recognizes Robert Sellers for his report for Enterprise Resiliency.

### 3. Enterprise Resiliency Update

**Mr. Sellers:** Good morning. My name is Robert Sellers, and I am the Chief Technology Officer for Citizens. I report to Kelly Booten and my primary areas of responsibilities include our Enterprise Architecture, IT Strategy, Enterprise and IT Resiliency, and IT Security & Risk.

This past June, we briefed you on the recent updates to the IT Strategic Plan. Today, as part of our primary responsibilities to the committee, we are providing a briefing to the committee on our Enterprise Resiliency and IT Security & Risk statuses.

We will start off with our Enterprise Resiliency program. Since March of this year, we have been utilizing different facets of the program as part of our COVID-19 response. What is our Enterprise Resiliency definition? Enterprise Resiliency is the ability to anticipate, absorb, respond to, and mitigate negative

impacts to the business from unexpected crisis events and business interruptions. At Citizens, the Enterprise Resiliency program establishes the methodology, the processes and the procedures required to continue the services to our policyholders in the event of a business interruption.

How do we determine what the scope of the program should be? We do this through a business impact analysis process. That means we look at all the business areas to identify what the critical processes are to develop solutions and to continue to provide those services.

Slide two – the completed Business Impact Analysis specifics provides us with the significant processing details of the business. It helps our Enterprise Resiliency team, for which I have three people scattered across managing the program, an individual focused on business continuity and an individual focused on IT disaster recovery. Sandy Allison manages that department. This helps our Enterprise Resiliency team understand what the processes are, how they are done, the people that are needed, the technology required to support it, and other resources required, along with the interdependencies.

One of the major objectives of the Business Impact Analysis is to determine what the Recovery Time objectives are for the systems that support our business activities. To do this, we conduct the Business Impact Analysis on the worst-case scenario for our organization. For us, the worst-case scenario would be a major event to a facility, to our people or to our technology platforms that takes place while we are managing a CAT event. This helps us determine what the impacts might be and what the maximum allowable time the business can tolerate being unable to perform different critical processes.

Once we determine what those recovery objectives are, we then look at different strategies that are in place to mitigate the impact of not being able to perform different business tasks. We identify any gaps that may exist, and then we help the business units to mitigate the impacts by working with them on implementing alternative strategies.

The latest Business Impact Analysis identified the mission critical processes that we utilize to provide services to our policyholders, the time in which they must be available, and the 34 mission critical systems supporting those processes that must be available or recovered within 24 hours or less. There are a number of them that have to be available within eight hours.

In addition, the Business Impact Analysis identified the people that we need over a specific period of time to support the continuation of the business processes, the operational equipment that is required (we have very specific hardware around our check processing and other equipment), the supplies that are necessary for those, along with other interdependencies between those business processes and our third-party business partners.

On the next slide - Enterprise Resiliency Governance. This program is considered operational. We went through a build stage where we were continuing to focus on the entire program, what was needed, and then putting that in place across the organization. Today it is considered an operational program and is part of our daily operational activities. We continually are making improvements in these processes through lessons learned from our exercises, assessing our state of readiness, and the actual events that occur.

Quarterly, an Enterprise Resiliency Governance Committee of senior leaders meet where we present the status of the program, the activities that are planned, and the timing of those so that the different business

units understand where they will need to coordinate their activities to maintain their plans and participate in those exercises by identifying any concerns or improvements for which the committee can provide guidance.

This year with COVID, the Crisis Management Team Red Book was reviewed and revised to include lessons learned from a Crisis Management Team exercise that was conducted on March 11th, just before COVID activities started, and from actual COVID-19 response activities that we have had since. Additionally, there were some management changes in the first part of the year that triggered plan updates.

The next slide is Business Continuity. At the beginning of the year we had 18 different business continuity plans that formed an umbrella of Enterprise Resiliency for the organization. With the reorganization of several business units this summer, we now have 19 different business continuity plans.

With all the ongoing activities related to COVID-19 response, the business continuity annual planning maintenance was delayed; it then began in July with an anticipated completion by October. Next year, as part of the resiliency plan improvement, the continuity plan reviews and updates will occur in the first half of the year prior to storm season.

Let's go to the next slide – Business Continuity Exercises. Annually, we conduct various business continuity exercises and resiliency state assessments. In 2019, these were completed with teams for all 18 business continuity plans. From the exercises and observations, recommendations for improvements were provided to the business for their consideration and plan updates. Along with plan exercises, the Resiliency State Assessment determined that the resources, the procedures, and the resiliency practices are in place, and it measured the competence of the business unit teams ability to manage an interruption. This is all about each individual business unit, in tandem with the rest of the organization, being able to manage through an event, come out the other side, executing on their processes.

Our overall state of preparedness for the enterprise was a little over 95 percent, which means we have essentially what we need to respond in the necessary time frames to an event. Our confidence level was at 86 percent with indicators showing that we need additional resiliency training for our teams. Additional training with teams occurred in some areas immediately after the exercises, while other training opportunities occur through regularly scheduled exercises and continued process improvements. And, of course with COVID this year, we have been exercising lots of different pieces of our business continuity plan.

In April of 2019, we had the opportunity to test with Agility Recovery Solutions, our vendor that we contract with for space in the event of a building being unavailable (less critical today), or if technology resources are needed to support our users. A Mobile Recovery Unit was brought into Tallahassee where most of the business units were able to participate and determine their ability to continue operations using those services. The exercise was successful and, as always, improvement opportunities were identified, and additional strategies were implemented.

The schedule at the bottom right of the slide shows our 2020 exercise schedule which kicked off in August of this year.

On slide seven, we will talk a little bit about COVID-19. This has been, not only for our organization, but for many businesses across the state of Florida and across the world, the major defining business continuity event of our past. Recent activities for the COVID-19 response and our COVID-19 workgroup have included developing and validating alternative strategies for maintaining the CDC guidelines for field staff, monitoring and providing ongoing support to essential staff that remain in our buildings, of which we have about 30 individuals today, and assessing third-party vendor risk areas.

In addition, we continue to raise awareness and enhance processes in assisting our employees with their personal preparedness if an evacuation were to be required during a storm. The CDC continues to provide guidelines for those who may have to evacuate, which have been communicated and are posted to our internal portal for staff awareness.

On slide eight, we talk about our Disaster Recovery. As Kelly mentioned, we have gone through exercises this year, and I will talk a little bit further about the exercise programs, but our IT Disaster Recovery Readiness for systems availability and recovery is solid today. We have continued to reduce the likelihood of needing it with further stability and availability enhancements to hardware, software, IT and business processes, by the IT Services and Delivery teams under Aditya Gavvala.

These improvement activities have also helped with the development of a roadmap to implement the infrastructure part of our cloud strategy, which will begin with moving parts of the Winter Haven disaster recovery infrastructure to the cloud. It's important to look back at the past as we look at accomplishments of this year and into the future.

In 2019, we conducted our annual Citizens Insurance Systems (CIS) exercise and reduced the time to complete the failover by approximately two hours. During that exercise, the business was able to validate the ability to complete the business processes in the Winter Haven facility and to validate the success of returning systems back to the production environment at the CSX Data Center in Jacksonville.

This year, the annual CIS exercise conducted on July 11th, again was successful and provided us the opportunity to demonstrate continued improvement in which we, again, reduced our failover and recovery time frames by almost an additional two hours. As Kelly mentioned, the Office of Internal Audit participated in the exercise and provided an Advisory Memo in which they agree with our conclusion that the exercise met the failover and recovery plan objectives.

Additionally, there are exercises planned for 2020 to validate additional key systems, and we continue to conduct specific unit testing and health checks on new technology as it is put in place, and existing systems as we complete enhancements.

We will finish on the last slide – CAT Assurance and Response. As you are aware, we are in the middle of the 2020 storm season. Our CAT Assurance and Response validation process is conducted annually. This year we tracked over 140 items which allowed the teams to validate the readiness of our system capability, processes, and people to support our policyholders and other stakeholders during a storm event.

Our field service vehicles and other supporting services are deployment ready. Additionally, technology and business enhancements this year include the ability to provide Additional Living Expense payments to our policyholders via an Electronic Funds Transfer process, shortening the time frame for those payments.

Modifications were also completed to address the enhanced services for the Catastrophe Response Center deployment based on the CDC guidelines.

The impact of COVID-19 required us to pivot and leverage more significantly different virtualization technologies such as Citrix, Softphones, and other solutions to enable independent adjusters to work remotely and effectively, minimizing the need for them to be on-site to support business and to be best able to respond to policyholders during a storm.

Mr. Chairman, this concludes my briefing on the state of our Enterprise Resiliency Program and the specific areas that fall within its domain. If there are any questions, I will take those at this time.

**Chairman Holton:** Thank you, Robert. Questions for Robert?

**Mr. Foley:** Hey Robert, this is Brian. I want to tie together what Kelly reviewed and what you are looking at here for business continuity with some of the things that we are struggling with. Particularly with audits, and not specifically business continuity, but more generally availability, which ties into business continuity, in that the audit windows are closing, particularly with SOC2 and OIG, and for us CMS, where they are requiring much more rapid implementation and closing of vulnerabilities in tighter, tighter windows; it's gotten us to the point where we have said that we can almost no longer just maintain the traditional view of business continuity, but we have got to get more towards hot, hot or critical items, critical applications, because the doing stage and development and test and production in 15-day windows when a critical vulnerability comes out just does not work in the traditional model. Are you all thinking about that?

**Mr. Sellers:** Brian, we are, and part of the cloud strategy is to allow us to move towards always on, always available type systems. Today, we are using parts of technology around database called Always On Technology to keep copies and availability of database in multiple locations, both in Jacksonville and in Winter Haven.

As we move to the cloud, and move the disaster recovery capability to the cloud, and then further on move our production to the cloud, the idea is to get to availability being confirmed, as close as possible, to 100% availability. The business processes today are so critical we really are technology organizations that do insurance, in some cases, where the technology just has to be there in order for us to do processing. I think that is true in many organizations.

And so that is the direction we are headed, as well - the always on, always available – a very rapid turn around and response, if we were to have a failure.

**Mr. Foley:** Yes, and that completely changes what you view as disaster recovery, because you are always ready.

**Mr. Sellers:** Yes, it does.

**Chairman Holton:** Thanks. Any other questions for Robert on this item? Okay, thank you, Robert. None being heard, let's move on to item four, and Robert you are still recognized for the IT Security & Risk Update.

## 4. IT Security & Risk Update

**Mr. Sellers:** Okay, thank you. Members of the Committee, today I've requested our Director of IT Security & Risk, Carlos Rodriguez, to undertake this briefing on the security and risk topic. As many of you are aware, these are to say "interesting times" in the space of technology and information security and risk.

Carlos leads a team of experts focused on both of these areas within IT. We have a strong partnership with many parts of our organization, including our legal privacy team, our Enterprise Risk team, the Office of Internal Audit, and our Inspector General's Office, and of course, all of IT were involved in the delivery of these services. And with that Carlos, please go ahead with your report.

**Mr. Rodriguez:** Thank you, Robert. Good morning Governors and Advisers. For the record, my name is Carlos Rodriguez, and I am the Director of IT Security & Risk, responsible for strategic and day-to-day activities related to IT Security, Incident Response, and Risk and Compliance Management for IT.

As always, I would like to remind you that detailed briefings on our specific security and risk activities with any of the Technical Advisers or Board members are always available at your request.

First, I would like to take the opportunity to remind you all of why we exist as a department within Citizens. We are here to support all divisions and departments of the organization to produce business outcomes by providing advisory services that seek to balance risks; and hopefully, avoid taking on undue technology risk by protecting the confidentiality, integrity and availability of our assets.

Slide three: We do this through the implementation and monitoring of eight different objectives set up in 2018, which you can see on the far right of the slide. We completed this strategy by connecting the Security Program Goals to the Enterprise Strategic Goals. This was one of the very first exercises we completed when I first joined Citizens to help us all understand how we integrate across the different efforts of the company. This chart has also become a powerful tool for me to help my team and others to see their connection to purpose.

Slide four: We have been on a journey to align our program with a three lines of defense approach because of two reasons: one is that our Office of Internal Audit follows this model for managing risks across the enterprise, and second, it clearly helps us communicate that risk is a shared responsibility across the organization and that everyone plays a role in it.

So, when you are looking at the pyramid, from bottom up going right to left, we have the many operational activities that take place at each line. And again, it highlights the roles and responsibilities of operational teams, risk management teams and the executives.

Business and IT Operations management own the security controls and risks, and serve as the first line of defense, as you can see at the very bottom of the pyramid. They work closely with IT Security & Risk and Enterprise Risk Management to implement and maintain effective operational controls.

IT Security & Risk serves as the second line of defense with close support from our Enterprise Risk Management and privacy teams, establishing and implementing the information security vision, program

management, enterprise policies and standards, control design and information security risk management while providing oversight, support, monitoring and reporting of the operational controls.

The Office of Internal Audit serves as the third line of defense, at the top of the pyramid, providing independent and objective assurance, and validating the effectiveness of the operational controls and overall risk management framework while keeping the Executive Leadership Team and Board of Governors informed to make educated IT and security risk management decisions within Citizens' risk tolerance levels.

Then going down from the top of the pyramid, we see that our executive team sets the tone, risk tolerance and direction that we all put into practice through implementation of our frameworks, standards, and policies that govern our IT and security program.

In addition, as you can see to the right of the pyramid, we also have external stakeholders who also bring independent assurance to our program. These entities include the Auditor General of the State of Florida, the Office of Insurance Regulation, and external financial auditors, all of whom compliment the work conducted by our Office of Internal Audit, our Enterprise Risk Management, and many self-initiated third-party reviews of specific areas of our operation, focused on data and operational security and risk.

On the last slide I am going to review with you some of the improvements that we have made over the last couple of years. These improvements, I want to emphasize, have not been the doing of IT Security & Risk alone; there has been significant work done by and partnerships with different IT teams, the Enterprise Architecture team, our Vendor Management Office, our Privacy team, and again, our internal Office of Internal Audit, with great support and collaboration by all business units.

Let's start with Identity and Access Management. Sarah Harrell will provide an update on our program in a little bit, but I would like to highlight a couple of the program's operational achievements. We have addressed many access-related risk and compliance matters through the revisions and roll out of processes and solutions, such as Multifactor Authentication, Privilege Access Management and Periodic Access Verifications, all areas which we continue to expand, mature and make progress on through new innovative solutions.

While we always focus on protecting our assets, incidents are inevitable in the business world today and our second objective is focused on Incident Response. One of the core components of our program is our ability to quickly detect and respond to events and incidents, which is also an area where we have matured rapidly by partnering with a Managed Security Service Provider that monitors all of our assets and access 24/7, improving our ability to respond to incidents from days to two hours or less. The results can be seen in that we have only had two real enterprise incidents over the last couple of years that we had to escalate to an Enterprise Incident Response level.

The other component of our response posture is our processes. We have an Enterprise Data Incident Response Plan that lays out the processes and response plans that we have followed resulting in effective engagement of all stakeholders and proper communication and collaboration. This plan is revised and tested annually.

There have also been significant improvements in all of our goals to mature our program. I will touch on some of them:

- First, we have been able to protect our assets with uninterrupted vulnerability and patch management activities as we transition to a remote workforce.
- We have developed a ransomware-specific runbook to quickly respond to such events.
- We also performed significant and very detailed work on risk and control identification and implementation for launching Microsoft Office 365 features such as Teams and others that are enabling our capabilities to support a collaborative remote workforce. That includes other cloud platforms, as well.
- In addition, we achieved major improvements on projects and operation risk and control assessments that have led to improvements within our Software Development Lifecycle.
- We also initiated our Information Protection and Data Loss Prevention program in support of our continued progress to cloud adoption.
- Great progress has also been made over the last 12-18 months in terms of speed of remediation of audit and compliance gaps while maintaining the number of new findings within manageable levels and minimizing the numbers of recurring issues. As was stated by Brian Foley earlier, we have the same challenge.
- We have ramped up our education and awareness efforts by introducing a monthly security newsletter, a new security awareness training platform, and the introduction of our Security Champion's Program to help application developers, IT professionals and business units learn about our program and security as a whole.
- And finally, we have moved to bi-monthly phishing exercises maintaining a low failure ratio while increasing the number of reports of phishing attacks, both simulated and real.

Governors, notice that I have left out any specifics on our technology in our environment. I want to remind you all that the results are available upon your request.

And Governors, this concludes my presentation. Thank you for your time and attention today.

**Chairman Holton:** Thank you, Carlos. Robert, any further comments or questions?

**Mr. Sellers:** No, sir. But as Carlos mentioned at the beginning, we are available at your request to do any type of personal briefings at any time. Thank you.

**Chairman Holton:** Thank you so much for that. Members, any questions for either Carlos or Robert? Okay, thank you guys for that great report.

We will move on now to item five, and the Chair recognizes Sarah Harrell for the identity and access management update.

## 5. Identity & Access Management Update

**Ms. Harrell:** Good morning, committee members. For the record, I am Sarah Harrell, the Director of Enterprise Programs responsible for the delivery of the enterprise multi-year initiatives. The deck for the Identity and Access Management Update is behind tab number five of your material.

On the next slide is a recap of the business objectives of the Identity and Access Management Program. You have seen this before. “Identity is the new perimeter” is the tag line of the program if you will.

Due to today's mobility and our ability to access information and resources on multiple devices, a simple ID and password is just no longer sufficient access control from a security perspective.

The business objectives of the program are listed there. I am not going to read them to you. The key one, though, is the first one listed, which is the reduction of cybersecurity risk - the mitigation of the risk of an incident or a breach.

On the next slide is the program update, and similar to this committee's last update, it will be brief and intentionally at a very high level due to the confidential IT security aspects and implications of the program initiatives. This is stipulated on the footer of this slide, but as Carlos and Robert both indicated, if any additional detail is required for any of the initiatives, we are happy to provide that in one-on-one briefings on request.

The program is using a common, two phase approach. First, an assessment to validate the strategy and develop an implementation roadmap, and then phased execution of that roadmap.

As you know the Gartner engagement for the strategy validation completed last year and the execution of the implementation roadmap is underway. Kelly Booten is our executive sponsor. Her delegate sponsors and program owners are Robert Sellers and Aditya Gavvala, both IT executives at Citizens.

This is a three to four-year program. We started it this year, so we expect it to run through sometime in late 2023 to 2024. The projected cost is $7.3 million, but that is just a proforma estimate, an order of magnitude estimate, if you will, from Gartner based on their industry expertise and metrics.

But, of course, the actual cost of the program will be driven by the vendors and the services selected and the spend approved by this committee and, ultimately, the Board of Governors.

The program execution also includes commitment to perform checkpoints every 12 to 18 months or as needed. In fact, because of the quickly evolving landscape in the IAM space, the first planned checkpoint was just accelerated based on Gartner industry intel that we received regarding an emerging trend that two of the tools that are currently on our implementation road map may be converging. So, with sponsor support, we paused to explore this trend and to assess it to determine if our roadmap and strategy required any updates. We are doing an internal assessment of those two tools potentially converging, and then we will engage an independent third-party to validate our assessment just to ensure that there is no unintentional bias to any products and to identify any glaring functionality gaps.

Based on the findings of that checkpoint, we will adjust the timelines, if needed, and that should occur in Q4. In fact, that will be the overall approach for these checkpoints that we do throughout the program, we will pause, assess, and recalibrate the timeline, as needed.

The program consists of five initiatives. The three green ones highlighted there are currently running in parallel. They had staggered start dates, but they are currently running in parallel.

And the first two, as Carlos alluded to, have already delivered functionality in iterative deployment phases, and the third initiative will have a longer timeline depending on what we find from our checkpoint and if there are any procurement needs required.

The timelines will be recalibrated as needed, not only based on our assessment checkpoints, but also just as the program progresses through this four-year implementation cycle.

Unless there are questions, that concludes my update.

**Chairman Holton:** Any questions for Sarah? None being heard, thank you for that report, Sarah.

We will move on to the final action item and the Chair recognizes Kelly Booten for that.

**6. Contracting Authority Request for 2021 Technology Needs (Part 1)**

**a. Technology Infrastructure, Software, and Professional and Staff Augmentation (Part 1) Action Item**

**Ms. Booten:** Good morning. Today I would like to request approval for contracting authority for the 2021 technology needs part one. Since 2009, Citizens has annually requested Board approval for technology, goods and services via single action or consent items.

Historically, Citizens requests have been presented to the Board in December, along with the annual budget, seeking contract authority for the following calendar year. However, this year Citizens is taking a two-part approach in an effort to provide further lead time, transparency, and opportunity for review and questions by the Board in alignment with the Board's request during the March 25th, 2020, Board of Governors Meeting.

The current action item part one is primarily focused on anticipated purchases in January through April 2021. Our current approach fulfills the request to bring purchases forward to Board meetings in advance.

A second action item, part two, will be primarily focused on anticipated purchases in the May through December 2021 time frame, and will be presented at the December 2020 Board of Governors Meeting.

Part one is predominantly run the business type purchases, whereas part two is predominantly project and/or big expenditures that happen later in the year. Our budget tends to have a lot of the run type expenditures early in the year.

The action item requests contracting approval in the amount of $15,397,676 under the following three spend categories: infrastructure, software, and professional and staff augmentation services. The estimated contract spend is $6,453,422 for infrastructure, $5,210,321 for software, and $3,733,933 for professional and staff augmentation services. The action item also includes more detailed breakdowns of anticipated expenditures in each of these three categories.

Contracting approval is requested for the list of contracts specified within the action item. These contracts are existing Citizens procured contracts and state term contracts and alternative contract sources approved by the State of Florida, Department of Management Services.

Funding for the requested contracts in the amount of $13,147,754 will be included in the upcoming 2021 budget request that will be submitted to the Board of Governors for approval in December 2021. For purchases having a contract term extending beyond 2021, funding for subsequent contract years will be budgeted in the appropriate year. There were five items within the detail that were multi-year contracts. We have a detailed backup that we can provide to you if you would like to have that.

If there aren't any questions, I can read the recommendation.

**Chairman Holton:** Members, any questions before Kelly reads the recommendation? Go ahead and read.

**Mr. Foley:** This is Brian Foley. I have one question for Kelly and team. One of the things that we have noticed with COVID is that for management and professional services with less of a requirement for folks being geographically located in the northeast Florida area, it has kind of opened up the aperture and we are looking at different types of contracts with different vendors that we normally wouldn't have considered now that we have proven that we can work productively remotely. Are you looking at that?

**Ms. Booten:** Yes, sir. Our opportunities are a little bit different than they used to be. The same thing with recruiting. We are looking at any option possible to bring in talent. And earlier when I reported on the GROW Program, we are even looking at bringing internal people into the program; every type of opportunity we can have to bring people in from different avenues we are looking at it, and that is one of them.

**Chairman Holton:** Brian, any follow up to that?

**Mr. Foley:** No, that is good. Thank you.

**Chairman Holton:** Okay. Members any other questions for Kelly before she proceeds to the action item? Okay, Kelly, go ahead, please.

**Ms. Booten:** Staff recommends that the Information Systems Advisory Committee[1] approve this action item totaling $15,397,676, and authorize staff to take any appropriate or necessary action consistent with this action item.

**Chairman Holton:** Thank you, Kelly. Do I have a motion to approve this action item?

**Brian Foley made a motion to approve the Technology Infrastructure, Software, and Professional and Staff Augmentation (Part 1) Action Item and John Vaughan seconded the motion. Roll was called. All were in favor. The motion carried.**

[1] Verbatim correction: although the recommendation should have been made from Staff to Information Systems Advisory Committee and not Information Advisory Committee to Board, this action item was moved for presentation at the September 2020 Board of Governors Meeting.

## 7. New Business

**Chairman Holton:** Okay, thank you. The next final item is new business. Is there any new business to come before the committee? None being heard, I will remind everyone that we will have a teleconference and we will be advised in the future when the date will occur, and staff will be in touch with you.

If there are no other comments, I will entertain a motion to adjourn.

**John Vaughan made the motion to adjourn. Meeting adjourned.**