CITIZENS
PROPERTY INSURANCE CORPORATION

Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

AUDIT REPORT

Third Party Access

March 28, 2018

Table of Contents: Page

Executive Summary

Appendix

Executive Summary

Background

Third party access refers to any non-employee or network that connects to Citizens' information assets including applications, services, infrastructure or data. Some third party relationships may involve critical business activities or access to confidential information.

Management of third party access and network connections is generally part of an overall third party risk management program and is a component of cyber security. Effective management of third party access includes understanding the risks that each party presents and implementing corresponding safeguards to reduce the risk of errors or malicious activities that may result in financial loss or business interruption.

Our assessment of a number of industry leading surveys over the last couple of years has indicated that third party activities are not being fully controlled in a large percentage of companies. Where not well controlled, the chance of a data breach occurring is significantly higher.

Within Citizens, the IT Security and Risk department is responsible for enacting policies and standards related to information security which apply to all users, including third parties. Information Security is also responsible for evaluating vendor (third party) security controls and for assessing Citizens' compliance with information security policies and legal requirements. The Vendor Management Office (VMO) is responsible for developing and maintaining governance structures as necessary to implement the Vendor Management Policy including developing standards, procedures and reporting requirements. The VMO has incorporated security and confidentiality provisions into the standard contract template.

Audit Objectives and Scope

The objective of this audit was to evaluate the adequacy and effectiveness of the processes and controls in place to manage third party access to Citizens' information assets such as data, applications, services and infrastructure.

The audit scope included the following components of the program:

- Governance structure
- Policies, standards and procedures
- Inventory and risk assessment of third parties
- User account management
- Logging and monitoring of third party activity
- Compliance assessments

Audit Opinion

The overall effectiveness of the processes and controls to manage third party access is rated as **Needs Improvement**.

Our work indicated that there are several opportunities for improvement associated with Citizens' management over third party access. These opportunities were discussed with IT management and included:

- **Clear assignment of governance ownership** to IT Security and Risk Department should be established. The responsibility for the governance over third party access and network connections has not been assigned to a single entity within Citizens. As a result, there may be a lack of consistency in managing third party access.

- **IT Security Standards need to be assigned to appropriate functions** responsible for implementation and ongoing management. In the absence of clear accountability there is a risk that some provisions may not be implemented and Citizens may not be fully protected from an incident facilitated by third party access.
- **The IT Security Standards need to be implemented** and monitored to completion. Work is underway to implement a portion of the standards associated with the Critical Security Controls framework; however, third party access controls are not included in this work. This lack of controls could also lead to unmitigated risks.

We would like to thank management and staff for their cooperation and professional courtesy throughout the course of this audit.

Appendix 1

Definitions

Audit Ratings

Satisfactory

The control environment is considered appropriate and maintaining risks within acceptable parameters. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern.

Needs Minor Improvement

The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed. Once the identified weaknesses are addressed, the control environment will be considered satisfactory.

Needs Improvement

The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully satisfactory. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory

The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses.

Appendix 2

Issue Classifications

Control Category	High	Medium	Low
Financial Controls (Reliability of financial reporting)	• Actual or potential financial statement misstatements > $10 million • Control issue that could have a pervasive impact on control effectiveness in business or financial processes at the business unit level • A control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in the financial reporting process	• Actual or potential financial statement misstatements > $5 million • Control issue that could have an important impact on control effectiveness in business or financial processes at the business unit level	• Actual or potential financial statement misstatements < $5 million • Control issue that does not impact on control effectiveness in business or financial processes at the business unit level
Operational Controls (Effectiveness and efficiency of operations)	• Actual or potential losses > $5 million • Achievement of principal business objectives in jeopardy • Customer service failure (e.g., excessive processing backlogs, unit pricing errors, call center non responsiveness for more than a day) impacting 10,000 policyholders or more or negatively impacting a number of key corporate accounts • Actual or potential prolonged IT service failure impacts one or more applications and/or one or more business units • Actual or potential negative publicity related to an operational control issue • An operational control issue relating to any fraud committed by any member of senior management or any manager who plays a significant role in operations • Any operational issue leading to death of an employee or customer	• Actual or potential losses > $2.5 million • Achievement of principal business objectives may be affected • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting 1,000 policyholders to 10,000 or negatively impacting a key corporate account • Actual or potential IT service failure impacts more than one application for a short period of time • Any operational issue leading to injury of an employee or customer	• Actual or potential losses < $2.5 million • Achievement of principal business objectives not in doubt • Customer service failure (e.g., processing backlogs, unit pricing errors, call center non responsiveness) impacting less than 1,000 policyholders • Actual or potential IT service failure impacts one application for a short period of time
Compliance Controls (Compliance with applicable laws and regulations)	• Actual or potential for public censure, fines or enforcement action (including requirement to	• Actual or potential for public censure, fines or enforcement action (including requirement to	• Actual or potential for non-public action (including routine

Appendix 2

Control Category	High	Medium	Low
	take corrective actions) by any regulatory body which could have a significant financial and/or reputational impact on the Group - Any risk of loss of license or regulatory approval to do business - Areas of non-compliance identified which could ultimately lead to the above outcomes - A control issue relating to any fraud committed by any member of senior management which could have an important compliance or regulatory impact	take corrective action) by any regulatory body - Areas of non- compliance identified which could ultimately lead to the above outcomes	fines) by any regulatory body - Areas of noncompliance identified which could ultimately lead the above outcome
Remediation timeline	- Such an issue would be expected to receive immediate attention from senior management, but must not exceed 60 days to remedy	- Such an issue would be expected to receive corrective action from senior management within 1 month, but must be completed within 90 days of final Audit Report date	- Such an issue does not warrant immediate attention but there should be an agreed program for resolution. This would be expected to complete within 3 months, but in every case must not exceed 120 days

Appendix 3

Distribution

Addressee(s) Robert Sellers, V.P., Chief Technology Officer

Copies **Business Leaders**

Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Systems & Operations Officer
Christine Turner Ashburn, Chief of Communications, Legislative & External Affairs
Aditya Gavvala, V.P. IT Services and Delivery
Stephen Guth, V.P. Vendor Management
Mark Kagy, Acting Inspector General

Audit Committee

Bette Brown, Citizens Audit Committee Chairperson
James Holton, Citizens Audit Committee Member
Senator John McKay, Citizens Audit Committee Member

Following Audit Committee Distribution

The Honorable Rick Scott, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Joe Negron, President of the Senate
The Honorable Richard Corcoran, Speaker of the House of Representatives

The External Auditor

Audit Performed By

Auditor in Charge	Gary Sharrock
Audit Director	Karen Wittlinger
Under the Direction of	*Joe Martins* *Chief of Internal Audit*