Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

CITIZENS
PROPERTY INSURANCE CORPORATION

AUDIT REPORT

Network Assessment

March 9, 2018

Report Number: OIA 2017-IT-06

Table of Contents: **Page**

Executive Summary

Background

Citizens' Legal Counsel engaged a third party firm to perform a network assessment and evaluate the strength of Citizens' deployed security processes that protect the company against cyber risks within the IT environment.

Cyber security practices generally require the evolution of protection policies and procedures as infrastructure changes occur, new threats are identified and new business needs arise. These practices serve to promote the integrity and privacy of customer and company data. Citizens' network security policies require risk assessments and ongoing industry standard vulnerability testing as well as contracting an expert to periodically perform testing by simulating malicious external and internal attacks to determine potential security weaknesses. Test results are risk assessed, providing an opportunity for IT Management to enhance security processes and protection mechanisms such as architectural and configuration changes, access controls, vulnerability patching and/or updated operating system and software versions in order to better align with risk tolerance levels.

The Information Security department oversees Citizens' cyber security policies and the performance of network testing processes including vulnerability testing, social engineering testing and contracting services to conduct periodic independent penetration assessments. Anomalies detected through testing are provided to the appropriate infrastructure groups for remediation or exception processing. Third party penetration testing of Citizens' network was last conducted in 2014.

Audit Objectives and Scope

The objective of this audit was to evaluate the effectiveness of the processes comprising periodic network penetration testing. The scope included an assessment of the IT Security policies and standards associated with periodic penetration testing. As well, the third party test was assessed against Citizens' internal cyber security standards as well as industry leading practice standards and included the following components:

- Concept proposal objectives and scope
- Third party vendor contract and statement of work verbiage
- Test scope
- Test results
- Management's remediation plan

Audit Opinion

With our participation throughout the independent vendor network assessment, we confirmed that a detailed and comprehensive set of tests were conducted by the vendor and are of the opinion that the policies, standards and overall effectiveness of the testing process are rated as **Satisfactory**.

After completion of the test, the vendor provided a detailed report which described each test performed and the results from these tests. The report indicated that although no active exploits were identified, a number of security risks, including some opportunities for improvement, were illuminated. None of these risks were assessed as being critical deficiencies but are of a nature that require consideration and remediation. Management and IT staff developed a comprehensive plan for remediation of the issues noted. A copy of this plan was presented to OIA and we are of the opinion that in completing the planned corrective actions, appropriate attention will be given to the known vulnerabilities. OIA will monitor execution of the noted actions and report progress through the open items process.

Executive Summary

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

Management Response

Thank you for the level of engagement provided by the Office of Internal Audit during this activity.

Management has assessed this report and the opinion and is in agreement with the observations and opinion of the Office of Internal Audit. The Information Technology department has developed a time specific, priority based action plan to address the issues identified in the network assessment. Remediation progress will be monitored closely by multiple stakeholders, including Senior Systems and Operations Management, as well as the Office of Internal 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 3

Distribution

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

Copies

Business Leaders
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief, Systems and Operations
Dan Sumner, Chief Legal Officer & General Counsel
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Chuck Bowen, Counsel / Privacy Officer
Mark Kagy, Acting Inspector General

Audit Committee
Bette Brown, Citizens Audit Committee Chairperson
James Holton, Citizens Audit Committee Member
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

Audit Director	Karen Wittlinger
Under the Direction of	*Joe Martins* *Chief of Internal Audit*