REPORT NO. 2015-017
SEPTEMBER 2014

# INFORMATION TECHNOLOGY CONTROLS OF SELECTED SYSTEMS UTILIZED BY THE CITIZENS PROPERTY INSURANCE CORPORATION

## Information Technology Operational Audit


STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

## CITIZENS PROPERTY INSURANCE CORPORATION
## BOARD OF GOVERNORS

Members of the Citizens Property Insurance Corporation Board of Governors who served during the period of our audit are as follows:

| | |
|---|---|
| Chris Gardner | Chair from August 9, 2013 |
| Carlos Lacasa | Chair through July 31, 2013 |
| Don Glisson, Jr. | Vice Chair from July 19, 2013 |
| Gary Aubuchon | From August 2, 2013 |
| Bette Brown | From March 24, 2014 |
| Juan Cocuy | |
| Carol Everhart | Through July 31, 2013 |
| James Holton | From January 17, 2014 |
| Tom Lynch | |
| John Rollins | Through September 9, 2013 |
| Freddie Schinz | From August 2, 2013 |
| John Wortman | |

## PRESIDENT/CEO AND EXECUTIVE DIRECTOR

Pursuant to Section 627.351(6)(c)4.a., Florida Statutes, the Executive Director of Citizens Property Insurance Corporation is engaged by the Board of Governors, subject to confirmation by the Senate, and serves at the pleasure of the Board of Governors. The President/CEO and Executive Director who served during the period of our audit was Barry Gilway.

The audit team leader was Andrew Denny and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

# INFORMATION TECHNOLOGY CONTROLS OF SELECTED SYSTEMS UTILIZED BY THE CITIZENS PROPERTY INSURANCE CORPORATION

Information Technology Operational Audit

## SUMMARY

**This information technology (IT) operational audit was performed in connection with the operational audit of the Citizens Property Insurance Corporation (Citizens) required by Section 627.351(6)(m), Florida Statutes. The focus of this audit was limited to evaluating, for selected Citizens' IT systems, selected business process application controls over transaction data input, processing, and output; selected application-level general controls related to security management, system access, and configuration management; and actions taken by Citizens' management to correct the IT control deficiencies noted in our report No. 2013-011, Finding Nos. 10 and 11.**

**We will consider the effectiveness of Citizens' IT controls as evidenced by the findings included in this report, and summarized below, in the development of the planned audit procedures to be performed in conducting the operational audit contemplated by Section 627.351(6)(m), Florida Statutes.**

**Our audit disclosed areas in which improvements in IT controls and operational processes were needed. The results of our audit are summarized below:**

**Finding No. 1: Two users had inappropriate user access privileges to selected Citizens' IT resources without a valid business purpose.**

**Finding No. 2: As of the dates of our review, in excess of 19,000 user accounts had not been deactivated after a specified time frame of inactivity, indicating that Citizens' periodic reviews of user access privileges needed improvement.**

**Finding No. 3: Certain security controls related to selected Citizens IT systems' user authentication and logging needed improvement.**

## BACKGROUND

Pursuant to amendments made to Section 627.351(6)(a)2., Florida Statutes, Citizens Property Insurance Corporation (Citizens) was created to provide residential and commercial property insurance for applicants who are entitled but, in good faith, are unable to procure insurance through the voluntary market. It is to operate pursuant to a plan of operation approved by order of the Financial Services Commission, and is subject to continuous review by the Commission. Effective July 1, 2002, pursuant to those amendments, the policies, obligations, rights, assets, and liabilities of both the Residential Property and Casualty Joint Underwriting Association and the Florida Windstorm Underwriting Association became the policies, obligations, rights, assets, and liabilities of Citizens. In 2011, Citizens began a multi-year Core Insurance Solution implementation program to consolidate all lines of insurance onto a single integrated insurance platform that includes the Guidewire® suite of insurance applications (Citizens Insurance Suite), thereby replacing end-of-life legacy systems. In the conduct of its operations and statutory responsibilities, Citizens utilizes several information technology (IT) systems. Those systems include:

- The Citizens Insurance Suite that provides a complete set of systems to support underwriting, policy administration, billing, and claims management. The Citizens Insurance Suite is composed of three main components:
  - PolicyCenter® automates underwriting and policy management for personal and commercial insurance and is designed exclusively for property and casualty insurers. It is a complete system-of-record and

supports the core functions of the policy lifecycle including product definition, underwriting, quoting, binding, endorsements, and renewals. PolicyCenter® was implemented on November 4, 2013, for commercial policies and the target implementation date for personal policies is November 2014.

- ClaimCenter® is available for all property and casualty lines of business. ClaimCenter® enables end-to-end claims lifecycle management from dynamic, intuitive loss report intake through advanced adjudication processes and integrated operational reporting. ClaimCenter® was implemented on May 4, 2013, for commercial policies and was implemented on March 24, 2014, for personal policies.
- BillingCenter® is a billing and receivables management system. It automates the billing lifecycle, enables the design of a wide variety of billing and payment plans, manages agent commissions, and integrates to external payment systems. BillingCenter® handles agency billing for all lines of business and its dual-entry accounting core integrates with the general ledger. BillingCenter® was implemented on November 4, 2013, for commercial policies and the target implementation date for personal policies is November 2014.

- Legacy policy administration systems that are being phased out as the policies are migrated to PolicyCenter® include:
  - Electronic Policy Administration System (ePAS), which is a Web-based insurance policy administration system that allows authorized agents to quote and submit new personal lines policy applications, view policy statuses, and submit policy endorsements. ePAS includes personal, residential multi-peril accounts, as well as Wind high-risk accounts.
  - Wind System (Wind), which is an internally developed policy administration system created specifically for commercial wind damage coverage.
- Claims Tracking System (CTS) is a legacy claims management system that is being phased out as active claims are resolved and new claims are processed. CTS is used for sending and receiving claim assignments, monitoring claim handling processes, maintaining electronic claim files, and storing financials. CTS is being replaced by ClaimCenter® and only has a few remaining active claims.
- Credentialing Administration Information System (CAIS) is an automated tool developed by Citizens to track the status of deployment qualifications of vendor firms and personnel. Its primary purpose is to allow vendors to supply credentialing information and automate the review and approval process for all parties.
- Agent Appointment System (AAS) is a browser-based system used by agents applying for appointment to write Citizens' policies. AAS is designed to determine whether agents employed by contracted agencies meet the agent appointment requirements prescribed by law and adopted by the Board of Governors of Citizens.
- Property Insurance Clearinghouse (Clearinghouse) provides a multiple-carrier interface that identifies comparable coverage from participating private-market carriers before placing business with Citizens. Use of Clearinghouse is mandatory for all new Citizens HO-3 (Homeowners) Special Form policies effective on or after January 27, 2014. Clearinghouse will be expanded later to include renewal policies and additional personal lines policy types. Clearinghouse was developed and is maintained by a third-party vendor, Bolt Solutions, Inc.

## FINDINGS AND RECOMMENDATIONS

### Finding No. 1: Appropriateness of Access Privileges

Effective access controls include measures that limit user access privileges to IT resources to individuals with a valid business purpose, such as certain insurance agents and adjusters doing business with Citizens. External users accessing Citizens' systems as an agent must have an active agent license with an active appointment from Citizens to write Citizens' policies prior to being granted access privileges to Citizens' IT resources. External users accessing Citizens' systems as an adjuster must have an active adjuster license and work for one of the adjusting firms

contracted with Citizens prior to being granted access privileges to Citizens' IT resources. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

Citizens used the Citizens Authentication Gateway (CAG) as the central authentication method for the Citizens Insurance Suite and Clearinghouse. We selected 40 users with active user accounts in CAG and evaluated the appropriateness of user access privileges not only for the Citizens Insurance Suite and Clearinghouse but also for any additional user access privileges granted to ePAS, Wind, CTS, or CAIS. Our review disclosed that 2 of the 40 users had inappropriate user access privileges to the Citizens Insurance Suite, 1 of which also had inappropriate access privileges to ePAS. Specifically, 1 user, who was a licensed agent but did not have an active appointment with Citizens to write Citizens' policies, could create, edit, and view insurance policies within the PolicyCenter® component of the Citizens Insurance Suite and ePAS. The other user did not have an active adjuster's license but could create, edit, and view insurance claims and create payments within the ClaimCenter® component of the Citizens Insurance Suite.

Inappropriate user access privileges to the Citizens Insurance Suite and ePAS increase the risk that unauthorized disclosure, modification, or destruction of Citizens' data and IT resources may occur; and, in some instances, unauthorized adjuster payments may be made.

**Recommendation: Citizens should ensure that user access privileges to Citizens' IT resources are limited to individuals with a valid business purpose.**

### Finding No. 2: Periodic Review of Access Privileges

Effective access controls include deactivating user accounts that have not been utilized within a reasonable time frame. As part of its IT Security Computer Account Management, Citizens created a guideline for implementing processes to mitigate some of the inherent risk of granting access privileges to information resources. Some of the identified processes included periodic reviews of user accounts that had not been utilized for a specified time frame to determine whether the access privileges granted remained appropriate.

Although Citizens had identified processes and network IT controls to ensure that user access privileges were appropriate and remained appropriate, periodic review processes were not effective in deactivating accounts that had no recent activity in the CAG, ePAS, Wind, CTS, CAIS, and network operating system. Our audit determined that there were many instances where the user accounts with no activity for a specified time frame were not timely deactivated, indicating a lack of periodic reviews. As of the dates of our review, in excess of 19,000 user accounts had not been deactivated after a specified time frame of inactivity, indicating that Citizens' periodic reviews of user access privileges needed improvement. Without a comprehensive periodic review of user access privileges, the risk is increased that inappropriate access privileges may exist and not be timely detected.

**Recommendation: Citizens should improve the periodic reviews of user access privileges to all Citizens' IT resources to help ensure that the user accounts with access privileges that are no longer appropriate are deactivated.**

### Finding No. 3: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to user authentication and logging that needed improvement. We are

not disclosing specific details of the issues in this report to avoid the possibility of compromising Citizens' data and IT resources. However, we have notified appropriate Citizens' management of the specific issues. Some of the issues were communicated to Citizens' management in connection with our report No. 2013-011.

Without adequate security controls related to user authentication and logging, the risk is increased that the confidentiality, integrity, and availability of Citizens' data and IT resources may be compromised.

**Recommendation: Citizens should implement appropriate security controls related to user authentication and logging to ensure the confidentiality, integrity, and availability of Citizens' data and IT resources.**

## PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, Citizens had taken corrective actions for Finding Nos. 10 and 11 included in our report No. 2013-011 and applicable to the scope of this audit.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from February 2014 through May 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected IT controls for selected Citizens' IT systems during the period July 2013 through May 2014 and selected Citizens' actions taken through July 14, 2014. The focus of this audit was limited to evaluating: selected IT controls related to input, processing, and output for the Guidewire® insurance suite of applications (Citizens Insurance Suite), Electronic Policy Administration System (ePAS), Claims Tracking System (CTS), and Property Insurance Clearinghouse (Clearinghouse); the effectiveness of selected IT controls related to security management, system access, and configuration management for the Citizens Insurance Suite, ePAS, Wind System (Wind), CTS, Credentialing Administration Information System (CAIS), Agent Appointment System (AAS), and Clearinghouse, where appropriate; and the actions taken by Citizens' management to correct the IT control deficiencies noted in our report No. 2013-011, Finding Nos. 10 and 11.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective IT operational policies, procedures, or practices. The focus of this IT operational audit was to identify problems so that they may be corrected in such a way as to

improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of the audit, the audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Citizens' personnel.
- Obtained an understanding of the Citizens Insurance Suite, ePAS, Wind, CTS, CAIS, AAS, and Clearinghouse, including the purpose and goals, computing platform and related software, access controls and periodic reviews of access, data flow, external interfaces, and change management.
- Observed and evaluated the effectiveness of application access controls in appropriately restricting access to the Citizens Insurance Suite (PolicyCenter® as of April 22, 2014, ClaimCenter® as of April 28, 2014, and BillingCenter® as of April 21, 2014); ePAS and CTS as of March 24, 2014; Wind as of February 28, 2014; CAIS as of April 18, 2014; and Clearinghouse as of April 16, 2014. Specifically, we evaluated 40 active user accounts in CAG for appropriateness of user access for the Citizens Insurance Suite, ePAS, Wind, CTS, CAIS, and Clearinghouse.
- Observed and evaluated the appropriateness of logical access controls to the Citizens Insurance Suite, ePAS, CAIS, AAS, Clearinghouse, and the related network operating system.
- Observed and evaluated the effectiveness of Citizens Insurance Suite, ePAS, Wind, CTS, CAIS, and Clearinghouse access authorization procedures.
- Observed and evaluated the effectiveness of periodic reviews for CAG as of March 22, 2014; ePAS, CTS, and the related network operating system as of March 24, 2014; Wind as of February 28, 2014; CAIS as of April 18, 2014; and AAS as of April 9, 2014.
- Observed and evaluated the Citizens Insurance Suite and ePAS input, processing, and output control procedures that effectively promote the timeliness, accuracy, and completeness of insurance data.
- Observed and evaluated the effectiveness of change management processes and controls to ensure that Citizens Insurance Suite, ePAS, Wind, CTS, CAIS, and AAS program modifications are suitably authorized, tested, approved, and subsequently moved into production by an appropriate individual. Specifically, we tested 25 of 387 program modifications that were moved into production between July 1, 2013, and April 14, 2014.

- Observed and evaluated the effectiveness of the comprehensive configuration repository procedures for the Citizens Insurance Suite, ePAS, Wind, CTS, CAIS, AAS, and Clearinghouse.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

## AUTHORITY

Pursuant to the provisions of Sections 11.45 and 627.351(6)(m), Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

## MANAGEMENT'S RESPONSE

In a letter dated September 18, 2014, the President/CEO and Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

## EXHIBIT A
## MANAGEMENT'S RESPONSE

CITIZENS PROPERTY INSURANCE CORPORATION
2312 KILLEARN CENTER BLVD., BUILDING A
TALLAHASSEE, FLORIDA 32309

TELEPHONE: (850) 513-3700 FAX: (850) 513-3903

CITIZENS
PROPERTY INSURANCE CORPORATION

September 18, 2014

Mr. David W. Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Enclosed are the written statements of explanation from Citizens Property Insurance Corporation to the each of the findings of the preliminary and tentative audit findings from the information technology (IT) operational audit of selected systems as provided electronically by your office on August 18, 2014.

These written statements concerning the findings include current or proposed corrective actions. Our staff has worked through any initial questions that arose with your office in order to produce this document.

Should any additional questions or issues arise from this submission, please do not hesitate to contact Christine Ashburn at (850) 513-3746 or via email at christine.ashburn@citizensfla.com.

Regards,

Barry J. Gilway

Barry Gilway
President/CEO and Executive Director

Enclosure

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

**Finding No. 1:** Two users had inappropriate user access privileges to selected Citizens' IT resources without a valid business purpose.

**Recommendation**: Citizens should ensure that user access privileges to Citizens' IT resources are limited to individuals with a valid business purpose.

---

Management Response:

**Agent Access**
Agents are appointed to Citizens and credentials to IT systems are provided when:

- They have applied for and have been approved for an appointment with Citizens
- Citizens has validated that they have the appropriate insurance license in place for the line of authority they are applying for and the required appointments with eligible carriers as noted through the eligibility matrix
- They complete our new agent education program (on-line)
- They pay the applicable appointment fee, which is passed on to Florida Department of Financial Services (DFS).

An agent's credentials are removed from the system when:

1) Citizens is notified that an agent is voluntarily surrendering their appointment
2) Citizens takes action on an agent based on a violation of their agreement
3) Citizens is notified by DFS that an agent no longer has a valid license to sell insurance
4) Citizens audits the DFS records to determine if an agent still holds a valid license

Each of these actions are not automatic and can involve administrative delays between the time of notice/discovery and termination of system access.

For efficiency, Item 4 is not performed daily and that could also lead to a delay. Process improvements have been put in place to reduce delays and maintain a regular schedule for agent credential validation.

**Adjuster Access**
We reviewed reporting reflecting all ClaimCenter users including their groups and roles. We referenced these against CAIS to identify users with "adjusting" ClaimCenter roles that did not have an active license in CAIS.

The role of "Adjuster" was previously not limited to those individuals responsible for the adjudication of claims. Operational roles such as dispatch and administrative support were grandfathered into Claim Center with their historical permissions from CTS. Upon review and confirmation with the product owner, this is no longer valid and permissions have been updated for all users.

## EXHIBIT A (CONTINUED)
## MANAGEMENT'S RESPONSE

**Finding No. 2:** As of the dates of our review, in excess of 19,000 user accounts had not been deactivated after a specified time frame of inactivity, indicating that Citizens' periodic reviews of user access privileges needed improvement.

**Recommendation**: Citizens should improve the periodic reviews of user access privileges to all Citizens' IT resources to help ensure that the user accounts with access privileges that are no longer appropriate are deactivated.

---

Management Response:

We agree that deactivation of unused accounts after a specified time frame of inactivity is an effective control mechanism. The timeframe the audit used to calculate 19,000 inactive accounts may not be appropriate for the predominantly external user population accessing Citizens' systems, as the guideline referenced in the AG's report was changed but not updated in the process document.

Since the majority of Citizens' policy and claims systems users are external Insurance Agents, Claims Adjusters, Property Inspectors and Vendors, the process was changed to avoid disruption to external business users which would result due to the administrative requirements for re-activating accounts. Instead, each month IT Security provides user reports to Citizens' business units with information on the accounts in their applications, including periods of inactivity.

Citizens initiated the Identity and Access Management enterprise level program earlier this year for the purpose of improving Citizens' account management effectiveness. This will include establishing enterprise-wide roles, responsibilities, and accountabilities as well as establishing various identity and access management control requirements as applicable for internal and external users.

**Finding No. 3**: Certain Security controls related to selected Citizens IT systems' user authentication and logging needed improvement.

**Recommendation**: Citizens should implement appropriate security controls related to user authentication and logging to ensure the confidentiality, integrity, and availability of Citizens' data and IT resources.

---

Management Response:

IT Security will conduct a risk assessment of the selected systems. We will review the results and implement appropriate security controls to address the findings.