FINANCIAL SERVICES COMMISSION

RICK SCOTT
GOVERNOR

JEFF ATWATER
CHIEF FINANCIAL OFFICER

PAM BONDI
ATTORNEY GENERAL

ADAM PUTNAM
COMMISSIONER OF AGRICULTURE

OFFICE OF INSURANCE REGULATION

KEVIN M. MCCARTY
COMMISSIONER

October 19, 2011

Mr. Kevin M. McCarty
Commissioner of Insurance
Office of Insurance Regulation
200 E. Gaines Street
Tallahassee, Florida 32399

Re: Auditor General Report 2011-181, April 2011: Property and Casualty Insurers Financial Analyses Process and Information Technology Controls

Dear Commissioner McCarty:

Status information concerning corrective actions that have been taken in response to the findings that were documented in referenced report is provided in the attached documentation pursuant to Section 20.055(5) (h), Florida Statutes.

Sincerely,

Bonnie Deering
Inspector General

BD/db

Enclosure

cc: Audrey Brown, Chief of Staff
Joint Legislative Audit Committee

BONNIE DEERING • INSPECTOR GENERAL
200 EAST GAINES STREET • TALLAHASSEE, FLORIDA 32399-4211 • (850) 413-4975 • FAX (850) 413-4983
WEBSITE: WWW.FLOIR.COM • EMAIL: BONNIE.DEERING@FLOIR.COM

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030

Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
1 – Evaluation of Controls Over Insurer Financial Information	As part of its regulation and oversight responsibilities, OIR performs analyses of P&C insurer financial information. These analyses are used to monitor the financial condition of P&C insurers and to enforce the statutory provisions and applicable rules as they relate to the review of P&C insurer solvency. To perform these analyses, OIR utilizes insurer financial information provided by the NAIC. The NAIC administers the Financial Data Repository database (FDR) to, among other things, maintain insurer financial information and make it available to state insurance regulators. The information provided by the NAIC includes financial information that is required to be submitted to the NAIC both quarterly and annually by insurance companies. Some of the FDR information, such as insurance company risk-based-capital amounts and ratios, is considered confidential and, as such, is exempt from the State's public records laws. Information from the NAIC is provided to OIR through an information-sharing agreement associated with OIR's NAIC membership. As OIR routinely utilizes FDR information for the vital analyses of insurer financial conditions, OIR management must rely on the controls established by the NAIC to ensure the accuracy and completeness of the FDR information. In response to the AG's audit inquiries regarding OIR actions to evaluate the sufficiency of NAIC controls over the FDR and related information, OIR provided copies of certain representations made by NAIC staff concerning the effectiveness of the FDR controls. For example, NAIC staff asserted that NAIC runs validations on the data submitted by insurers to ensure the accuracy and completeness of FDR information. However, OIR had never sought an independent evaluation of, or requested an independent service auditor's report related to, the controls NAIC had designed and established for the FDR. Subsequent to the AG's audit inquiries, OIR contacted the	***OIR routinely obtain and review an independent service auditor's report on the effectiveness of NAIC controls established for the FDR and related information. OIR should consider the conclusions presented in the reports when utilizing the information provided by NAIC.***	As noted in the report, the Office has requested and expects to receive a service auditor's report pursuant to SAS 70 from the NAIC to cover the six-month period ending January 31, 2011. In addition, the Office would like to note that in an effort to ensure the NAIC FDR database is accurate and complete, the Office receives audited financial statements prepared by independent certified public accountant firms in PDF format. Office examiners and analysts compare the audited financial statements to the electronic filings of the insurer's annual statements in the FDR database and have found no inaccuracies or incompleteness in the FDR data. Correspondingly, Office examiners perform periodic onsite field examinations of insurers and compare the general ledgers and accounts of the insurers to the electronic filings in the FDR database. Office analysts are in constant communication with insurers regarding their data and the analytical process used to derive information in the FDR database. For example, it is common for analysts to follow-up with insurers on the risk based capital amounts, financial ratios, reserve development, asset and liability amounts for specific insurers. In fact, given the enormous detail of the data and review by our examiners and analysts, we are confident our efforts are tantamount to a verification of the accuracy and completeness of the FDR data. Ancillary to the above, the Office has run several reports from the FDR database and issued this information publicly, and have not encountered any insurers advising the Office of publishing incorrect data.	The Office received a copy of the service auditor report pursuant to SAS 70 from the NAIC. It appears that the NAIC has appropriate controls for the FDR and related information.	***CLOSED***

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030

Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
	NAIC requesting a service auditor's report. NAIC staff represented to OIR that its first SAS 70 engagement for the FDR was scheduled to cover the period August 1, 2010, through January 31, 2011, and that the resulting service auditor's report would be made available to OIR after the end of the first quarter of 2011. Absent a service auditor's report, or other independent evaluation of NAIC controls, OIR has limited assurance that the FDR information relied upon for the vital analyses of the financial condition and solvency of P&C insurers is accurate and complete.				
2 – Timeliness of Rate Filing Reviews	State law requires that, within 90 days of receipt of a "file and use" filing, OIR finalize its review by issuance of a notice of intent to approve or a notice of intent to disapprove. Requests for supporting information or corrections or notification to the insurer of its preliminary findings by OIR is not to toll the 90-day period. Should OIR not issue a notice of intent to approve or a notice of intent to disapprove within 90 days after receipt of the filing, the rate is to be deemed approved. The AG examined OIR review documentation for 38 P&C "file and use" rate filings and noted that OIR had timely issued a notice of disapproval for 6 of the 38 filings and a notice of approval for 28 of the filings. However, for 4 of the 38 rate filings, OIR had issued a notice of its decision more than 90 days after receipt of the rate filing. In each of these 4 instances, OIR approved the rate filings. In response to the AG's audit inquiry, OIR management indicated that the 90-day review period had been exceeded due to the need for additional information and that, for each of these 4 filings, the insurer had requested, in writing, an extension to the right to have the filing deemed approved. The AG noted that at least some of the insurer's requests	***OIR take appropriate steps to ensure the completion of rate filing reviews within the 90-day period established by law.***	In Gilman v. Butzloff, 22 So.2d 263 (Fla.1945), the Florida Supreme Court stated that "a party may waive any right to which he is legally entitled whether secured by contract, conferred by statute, or guaranteed by the Constitution." The Office (actually it predecessor-the Department of Insurance) issued Informational Bulletin 98-007 on October 28, 1998, a copy of which is enclosed, that outlines the position in regards to a waiver of deemer provisions. In the four cases described in the findings in which a waiver of deemer was received, the insurer decided it was in its best interests to waive the deemer to allow for additional time for review of the filing. It should be noted that, in all circumstances, this was due to the fact that the initial filing did not contain all information needed to review the filing. Thus, it required additional efforts by an Office actuary to determine whether the proposed filing complied with all applicable statutes and rules. The waiver of deemer was submitted by the insurer to avoid a Notice of Intent to Disapprove being sent by the Office. This allowed the company to		***CLOSED***

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030

Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
	had been prompted by an OIR request for additional time to complete the rate filing review. Notwithstanding the insurer's request for the extensions, it is unclear that OIR had the statutory authority to exceed the 90-day review period established by the law.		avoid resubmitting a complete filing to support the proposed changes, saving both time and effort. Since this protocol benefits both insurers and regulators, and improves processing time, the Office does not intend to alter its current procedure./		
3 – State Documentation for Rate Filing Decisions	Pursuant to State law, OIR actuaries and analysts are to review insurer rate filings to determine if a rate is excessive, inadequate, or unfairly discriminatory. In making that determination, OIR is to, in accordance with actuarial techniques, consider an insurer's past and prospective loss experience, past and prospective expenses, and the degree of competition among insurers for the risk insured. Actuarial standards require that records and other appropriate documentation be created to identify the data, assumptions, and methods used. The documentation of the data, assumptions, and methods used is to be sufficiently clear to allow another actuary qualified in the same practice area to evaluate the reasonableness of the work. In addition, NAIC guidance indicates that a rate reviewer should be able to explain specific actions taken on a rate filing and the impact of a rate change on business. The AG's evaluation of the process used by OIR staff to review rate filings disclosed that, while OIR staff documented responses to objective criteria when evaluating the reasonableness of a rate filing, OIR policies and procedures did not require that OIR staff document the reasoning, judgments, and calculations supporting those responses or the rate filing decisions made. For example, for one of the rate filings reviewed, explanations and computations supporting the approval of a percentage for prospective expenses that was lower than that submitted by the insurer was not documented. In response to the AG's audit inquiry, OIR management indicated that decisions	***OIR enhance its policies and procedures to require OIR staff to sufficiently document the basis for the reasoning and judgments made in support of rate filing decisions.***	The Office will review current policies and procedures in order to ensure all appropriate documentation is included in rate files.	Processes and procedures have been reviewed and the Office believes them to be adequate.	***CLOSED***

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030
Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
	were made by experienced and knowledgeable staff and were discussed among OIR staff at regularly scheduled meetings, although minutes or other similar records were not produced or maintained. An established policy or procedure requiring OIR staff to document, at the time of the rate filing review, the underlying reasoning and judgments affecting the decision would enhance OIR's ability to later explain specific actions taken regarding the rate filing and to support the reasonableness of the rate filing decisions made.				
4 – Conflict of Interest Forms	In accordance with State law, the OIR Code of Ethics requires all employees to annually sign Conflict of Interest forms affirming that they have no conflicts of interest related to insurers regulated by and entities doing business with OIR. The Conflict of Interest form is to be signed by the employee at the time of the employee's annual performance evaluation. The AG's test of OIR policies and records related to 23 OIR employees disclosed that, although OIR management revised the applicable AP&P based on a recommendation in report No. 2007-088, OIR management did not ensure that annual Conflict of Interest forms were signed by OIR employees. Specifically, a current signed Conflict of Interest form was not available in OIR records for 19 of the 23 employees. Subsequent to the AG's audit inquiry, OIR obtained signed Conflict of Interest forms from 18 of the 19 employees. OIR did not obtain a signed Conflict of Interest form from the other employee as she had separated from OIR employment on March 12, 2010. Obtaining employee affirmations that examinations, investigations, and other regulatory activities are conducted absent any conflicts of interest is critical to successful regulation as such affirmations provide OIR with assurances regarding the objectivity of regulatory personnel	***OIR management ensure compliance with State law and the OIR Code of Ethics by annually obtaining signed Conflict of Interest forms from all OIR employees.***	Current policy requires that a new conflict of interest form be signed and submitted at the time of the annual employee performance evaluation, and at the time of initial hire. However, in an effort to assure that all conflict of interest forms are completed timely, the Chief of Staff has amended this policy to require all forms be submitted by a date certain (currently April 1 of every year); rather than tying the form submission date to annual performance evaluations. In addition, the Conflict of Interest Form – Annual Certification of Adherence will be modified to reflect the new procedure. The Office believes this will resolve the issue.	Office management will amend the Conflict of Interest Form – Annual Certification of Adherence to reflect annual submission date of April 1st by Nov. 1st.	***OPEN***

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030

Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
	and activities. An undisclosed conflict of interest may bring into question the integrity of a particular investigation or examination, as well as, OIR's regulatory efforts as a whole.				
5 – FREDMS Access Controls	The AG's audit procedures disclosed that certain FREDMS logical access controls relating to the management of access privileges were deficient. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising OIR data and information technology (IT) resources. However, appropriate OIR personnel have been notified of these issues.	***OIR strengthen its IT security controls related to the management of FREDMS access privileges.***	Effective January 19, 2011, the Office instituted a process called Active Directory. This enhanced security measure now identifies each user and authorized roles at the point of logging on to your computer (the network) each morning. If the Auditor General's Office has any questions regarding this response, please contact Rebecca McCarley, Deputy Chief of Staff at (850) 413-5086.		***CLOSED***
6 – FAME Access Controls	As noted in report No. 2009-032, finding No. 2, certain FAME logical access controls relating to the management of access privileges needed improvement. The AG's follow-up procedures disclosed that, although OIR staff had taken some corrective action, deficiencies relating to certain FAME logical access controls continue to exist. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising OIR data and IT resources. However, appropriate OIR personnel have been notified of these issues.	***OIR strengthen its IT security controls related to the management of FAME access privileges.***	Effective January 19, 2011, the Office instituted a process called Active Directory. This enhanced security measure now identifies each user and authorized roles at the point of logging on to your computer (the network) each morning. If the Auditor General's Office has any questions regarding this response, please contact Rebecca McCarley, Deputy Chief of Staff at (850) 413-5086.		***CLOSED***
7 – AppCoord User Access Reviews	Effective security administration procedures include the periodic review of user access rights to reduce the risk of unauthorized system access. As noted in report No. 2009-036, finding No. 3, OIR staff acknowledged the lack of documentation demonstrating the conduct of a periodic review of Applications Coordination Document Management System (AppCoord) user access rights. OIR staff utilize the AppCoord to manage, track, and approve company applications to sell insurance in the State. DFS IT Security Policy and an OIR Chief of Staff memorandum dated October 31, 2007, direct OIR staff to	***OIR strengthen its IT security controls related to the management of AppCoord access privileges and establish a documented process for the periodic review and confirmation of user accounts, access controls, and privileges. The periodic review should be performed at least annually, or more frequently upon identification of a specific risk.***	Effective September 22, 2010, the Office instituted a process called Active Directory. This enhanced security measure now identifies each user and authorized roles at the point of logging on to your computer (the network) each morning. The Office has also instituted a user access review process. If the Auditor General has any questions regarding this response please contact Rebecca McCarley, Deputy Chief of Staff, at (850) 413-5086.		***CLOSED***

OIR/OIG AUDIT FOLLOW-UP REPORT

Audit Title: Auditor General Rpt 2011-181: Property and Casualty Insurers Financial Analyses Process and IT Controls – Six Month Follow-Up

Original Audit Project #: 09/10-030

Follow-Up Project #: C-1112OIR-018

Finding Number	Finding Summary	Recommendation	Management Response	Management Follow-Up	Status
	operate within DFS policy and procedures. The DFS IT Security Policy requires the periodic review and confirmation of user accounts, access controls, and privileges. The periodic review is to include, but is not limited to, a review of the user rights, restrictions, and password removals applicable to active employees and third parties. In response to the AG's audit inquiry, OIR management stated that, due to workload priorities during the 2009 calendar year, OIR staff again did not perform an AppCoord user access rights review. Subsequent to the AG's audit inquiry, OIR staff did conduct a user access rights review.				