



**Government of the District of Columbia
Department of Insurance, Securities and Banking**

**Stephen C. Taylor
Commissioner**

**BEFORE THE
INSURANCE COMMISSIONER OF
THE DISTRICT OF COLUMBIA**

Re: Report on Examination – Independent Statistical Services.

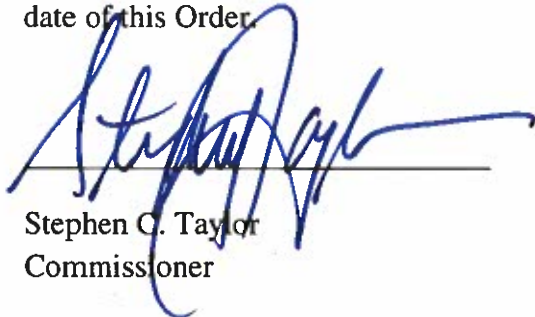
ORDER

A Market Conduct Examination of **Independent Statistical Services** as of December 31, 2017 has been conducted by the District of Columbia Department of Insurance, Securities and Banking (“the Department”) as a participating jurisdiction through the National Association of Insurance Commissioners Advisory Organization Examination Oversight (C) Working Group. The Department accepts the report in lieu of a single jurisdiction examination.

It is hereby ordered on this 7th day of January 2019, that the attached market conduct examination report be adopted and filed as an official record of this Department.

Pursuant to Section 31-1404(d)(1) of the D.C. Official Code, this Order is considered a final administrative decision and may be appealed pursuant to Section 31-4332 of the D.C. Official Code.

Pursuant to Section 31-1404(e)(1) of the D.C. Official Code, the Department will continue to hold the content of the report as private and confidential information for a period of 10 days from the date of this Order.



Stephen C. Taylor
Commissioner

Independent Statistical Service

Report of Examination
As of December 31, 2017

Multi-State Market Conduct Examination of
Independent Statistical Service

Table of Contents

I.	PURPOSE AND SCOPE OF EXAMINATION	2
II.	ORGANIZATION PROFILE.....	3
III.	EXECUTIVE SUMMARY	4
IV.	EXAMINERS' METHODOLOGY	4
V.	PRIOR EXAMINATION OBSERVATIONS AND RECOMMENDATIONS SUMMARY.....	5
VI.	REVIEW OF EXAMINATION STANDARDS	10
	A. CHAPTER 25 - OPERATIONS/MANAGEMENT/GOVERNANCE STANDARDS	10
	B. APPENDIX F OF CHAPTER 25 - MANAGEMENT AND ORGANIZATIONAL CONTROLS	14
	C. REVIEW OF STATISTICAL PLANS	19
	D. REPORTS, REPORT SYSTEMS, AND OTHER DATA REQUESTS	19
VII.	EXAMINATION SUMMARY	22
VIII.	EXAMINATION REPORT SUBMISSION	25

October 8, 2018

Director Jennifer Hammer
Illinois Department of Insurance
320 W. Washington St.
Springfield, IL 62767

Dear Director Hammer:

Pursuant to your instructions and in compliance with the provisions of Articles IX, XXIV and XXVI, Sections 132,401, 401.5, 402, 403, and 425 of the Illinois Insurance Code, and the procedures established by the National Association of Insurance Commissioners, an examination has been conducted of the market activities of:

**Independent Statistical Service
8700 West Bryn Mawr Avenue
Suite 1200S
Chicago, IL. 60631-3512**

hereinafter referred to as "ISS" or "Organization." The report of the findings of this examination is herewith respectfully submitted.

I. Purpose and Scope of Examination

A multi-state market conduct examination (the "Examination") of the Independent Statistical Service ("ISS or the Organization") was called for the period of January 1, 2015 through December 31, 2017 (the "Period"). The Examination was under the oversight of the Advisory Organization Examination Oversight (C) Working Group (the "Working Group") of the National Association of Insurance Commissioners ("NAIC"). Illinois served as the Lead State for the Examination. The Examination was in accordance with the Standards as set forth in the NAIC Market Regulation Handbook (the "Handbook") Chapter 25, and Appendix F to Chapter 25. The Illinois Department of Insurance (the "Department") retained Risk & Regulatory Consulting, LLC ("RRC or the Examiners") to assist in conducting the Examination.

The targeted focus of the Examination related to determining the Organization's compliance with applicable statutory and regulatory requirements, and specifically compliance with the findings of the prior examination of ISS as of December 31, 2012. Further, the Examiners were directed to identify and review any new matters raised by the Comprehensive Annual Analysis ("CAA") forms completed by ISS for the Period. The CAA assists in keeping regulators informed of Statistical and Advisory Organizations' activities with regard to the applicable Handbook standards as well as any changes in their business operations.

Finally, the Examiners investigated a specific request from the State of California, which is a Participating State, related to the Organization's process concerning the production of Fast Track Data and Experience Data Listings.

RRC personnel participated in this Examination in their capacity as Examiners. The Examination Team included Information Technology ("IT") Specialists and Market Conduct Examiners. RRC provides no representations regarding questions of legal interpretation or opinion. Determination of findings, if any, constituting potential violations is the sole responsibility of the Department. Failure to identify unacceptable or non-complying practices does not constitute acceptance of these practices.

II. Organization Profile

ISS, based out of Chicago Illinois, conducts business in all 50 states, the District of Columbia and Puerto Rico, under the authority granted by each jurisdiction. The Organization provides data and related information and reports to the NAIC and state insurance regulators, as well as other industry organizations. The National Association of Independent Insurers (“NAII”) created ISS to serve as a department within NAII to provide statistical reporting services to property and casualty insurers in 1947.

In July 2003, ISS became a separate incorporated wholly owned subsidiary of NAII. In January 2004, NAII merged with the Alliance of American Insurers (“AAI”) to form a new trade association known as the Property Casualty Insurers Association of America (“PCI”). As a result, ISS became a wholly owned subsidiary of PCI. It is important to note that PCI provides ISS with operational support to the Organization on a shared platform. The Examiners discuss this matter further in the report.

ISS publishes 15 state approved statistical plans for their subscribers. The Organization’s primary products are the annual statistical compilations, which are reports filed by line of business with regulatory authorities that fulfill the basic statistical reporting requirements on behalf of ISS’s reporting companies. For insurers writing private passenger auto and homeowners coverage, ISS offers Fast Track Plus, designed to assist the companies to monitor emerging claim experience on a quarterly basis. Additionally, Fast Track Plus trends information over multiple years.

ISS provided the information noted in the below table, which identifies the number of individual filings reported by year. The change in the Organization’s filings for the Period has been nominal.

Experience Year	Filing Year	# of Filings	% Change
2014	2014-2015	17,525	2.4%
2015	2015-2016	17,971	2.5%
2016	2016-2017	17,817	(0.9)%

The chart below displays the statistical filing years and the associated billing year. The revenue for billing years 2015 – 2017 has been stable and is consistent with the Organization’s filing history.

Filing Year	Billing Year	% Change in Revenue
2014-2015	2015	1.4%
2015-2016	2016	1.3%
2016-2017	2017	(3.9)%

III. Executive Summary

As commented above, the focus of the Examination was to determine the Organization's compliance with applicable statutory and regulatory requirements, investigate compliance with findings from the prior examination, and to investigate any new matters raised by the Working Group's CAA form completed by ISS for the intervening years. The scope of the prior examination focused on the Organization's processes and procedures, including but not limited to: Operations and Management; Statistical Plans; Regulatory Licensing or other authorization; overall Data Management and controls; correspondence with reporting insurers; report submissions to regulators; as well as compliance with Chapter 25 of the Handbook and its Appendix F.

Throughout the course of the Examination, the Examiners provided updates to the Lead States and the Working Group about the progress and findings of the Examination.

IV. Examiners' Methodology

The Examiners conducted interviews with ISS representatives, reviewed documentation provided by the Organization, and conducted on-site walkthroughs of the Organization's operations, which included a high-level review and testing of the relevant aspects of the Organization's IT infrastructure and controls. The Examiners also spent time onsite at ISS' offices in Chicago, and met with the Organization's Senior Vice President & General Manager and members of her staff.

Throughout the course of the Examination, Information Data Requests ("IDRs") were submitted to ISS to request information and/or to seek clarification of a particular matter. The Examiners, the Lead States, and ISS actively communicated throughout the course of the Examination to discuss progress and the overall status of the Examination. Additionally, the Examiner in Charge ("EIC") reported the status of the Examination to the Working Group during NAIC meetings. The Examiners discussed possible findings identified during the Examination with ISS, and in some instances, the Organization was able to provide additional information for the Examiners' consideration.

V. Prior Examination Observations and Recommendations Summary

As previously noted, the primary objective of the Examination was to determine the Organization's compliance related to the Examiners' findings and observations resulting from the prior examination. The following chart summarizes the Examiners' follow-up assessment. The Examiners have also provided additional details further in the Report regarding each prior observation.

Standard	Observation from Prior Examination	Organization's Response and Actions	Current Examination Follow-Up
<p>1. <u>Operations/Management/Governance Standard 12:</u> The advisory organization has an up-to-date, valid internal or external audit program.</p>	<p>The Examiners determined ISS does not have an internal audit function nor do they perform internal audits of its operations, including audits of internal statistical data and information systems.</p>	<p>ISS responded to the Examiners recommendation by noting: "The ISS board, at its July 14, 2013 meeting, implemented an external audit program to include an audit of financials, IT and statistical reporting under the oversight of the Audit Committee. At its July 15, 2013 meeting, the Audit Committee approved the program and the inclusion of ISS as a standing agenda item for each meeting to ensure regular consideration."</p>	<p>Based on the follow-up review the Examiners concluded that ISS does have an audit program; however, the Examiners identified additional recommendations to further enhance the audit program.</p>
<p>2. <u>Application Management Standard C.1:</u> Is there a control that ensures that user needs result in appropriate program change requests and the requests are properly developed?</p>	<p>The Examiners confirmed that changes to the statistical reporting applications are tracked in a Lotus Notes database. In addition, an internally developed system, Change Management System, is used for promoting statistical reporting source code and system functionality changes from the environment that is used to test these changes to its production environment. An effective change management process will address</p>	<p>At the conclusion of the prior examination, ISS responded by noting: 1. Change Testing Evidence: ISS has expanded its user acceptance testing process to include the retention of the test results that was the basis for user approval. Test results will vary by the scope and complexity of the project and could include screen, report and/or data samples. ISS implemented the retention of the test results on July 1, 2013. 2. Application Migration Approval: ISS has expanded its</p>	<p>The Examiners determined the Organization is in compliance with the Standard.</p>

Standard	Observation from Prior Examination	Organization's Response and Actions	Current Examination Follow-Up
	<p>requests for system changes, change review and approval, code development, review and migration procedures, and post implementation monitoring. However, there was no evidence that the Organization has a process of change testing or maintains migration approval.</p>	<p>migration process to include management review of recently completed migrations to ensure that the migration approval has been documented in the Change Management System.</p>	
<p>3. <u>Operations/Management/Governance Standard 17:</u> The advisory organization is appropriately licensed.</p>	<p>License renewal was sent to all 50 states, Puerto Rico, and the District of Columbia. Many states do not send any type of response. 9 states issued an actual license, while 5 states only sent a confirming note.</p> <p>Where a jurisdiction does not issue a license, ISS relies on two other sources as evidence of the jurisdiction's acceptance of ISS license renewals: (1) the canceled check for those states that impose a licensing fee and (2) acceptance of ISS state compilations.</p> <p>For jurisdictions in category (2) above, ISS maintains either a record of electronic acknowledgements of receipt for state compilations submitted to jurisdictions at their prescribed email address or acknowledgements of delivery from the USPS.</p>	<p>ISS responded to the Examiners' recommendation by noting: "ISS has confirmed the Organization has reviewed its current process and has added a process to contact States that do not acknowledge licensing or confirm receipt of reports."</p>	<p>The Examiners determined the Organization is in compliance with Standard 17.</p>

Standard	Observation from Prior Examination	Organization's Response and Actions	Current Examination Follow-Up
<p>4. <u>Logical and Physical Security Standard B.6</u>: Does user department management periodically validate the access capabilities provided to individuals in the department? Please provide evidence of the last user access review performed during the period under review.</p>	<p>The Examiners noted that a periodic review of user access, which would ensure that individual user access remains appropriate, is not formally performed nor documented. Consequently, the Examiners note that the Organization is not compliant with the requirements for B6 and B14 since periodic access reviews are not formally performed.</p>	<p>ISS responded to the Examiners recommendation by noting:</p> <p>1. Mainframe Environment - For the mainframe environment, ISS is implementing a process for management review of user access across the LPARs (test and production) that will include: Distribution of access rights for each active person, by the security administrator, to the appropriate department manager; Review and signoff of the access rights for each person by department manager; Retention of the signoff in the security repository.</p> <p>ISS will complete this assessment annually in January, to align with the assignment planning process. This process will be completed during the 2nd half of 2013, with implementation January 1, 2014.</p> <p>2. Statistical Reporting Systems - For the statistical reporting system, ISS is revising its security administration application to retain the appropriate documentation of the annual review currently done for active staff. This process will result in the following: Retention of the planned assignments for the new year; Online modification of individual access rights based upon project assignments by the appropriate project manager(s); Online review and signoff of all access rights for each person by the department manager, based upon the planned assignments for the year; Online access to the history of annual changes and department management signoff.</p> <p>ISS will complete this assessment</p>	<p>The Examiners concluded ISS has an adequate access review process in place; however, it was determined that PCI, which supports the Organization, does not review user accounts on a periodic basis. In addition, the IT Examiners noted that PCI does not periodically review the access listings for the doors and IT rooms. Therefore, ISS was determined not to be in compliance with the standard.</p>

Standard	Observation from Prior Examination	Organization's Response and Actions	Current Examination Follow-Up
		<p>annually in January, to align with the assignment planning process. Development and testing of the new online signoff process will be completed during the 2nd half of 2013, with implementation January 1, 2014.</p>	
<p>5. <u>Logical and Physical Security Standard B.14</u>: Are periodic checks carried out to confirm that employees' current application access is commensurate with job responsibilities?</p>	<p>See row 4 above. (Standard B.6)</p>	<p>See row 4 above. (Standard B.6)</p>	<p>Standard B.14 is linked with Standard B.6; therefore, the Organization is not in compliance with this Standard.</p>
<p>6. <u>Logical and Physical Security Standard B.19</u>: If wireless technologies are deployed, does the company monitor for rogue access points.</p>	<p>The Examiners discussed with ISS the Organization's use and monitoring of wireless access points for network access. Through the Organization's response to data requests regarding ISS system audits and reviews, it was determined that ISS does not periodically monitor for rogue wireless access points.</p>	<p>At the conclusion of the prior examination, ISS responded to the Examiners recommendation by noting:</p> <p>"PCI security staff is performing monthly scans of the headquarters facilities to identify any rogue access points that may be attached to the PCI network. This was implemented on 5/6/2013 and added to the IT Security Policy Document."</p>	<p>The IT Examiners determined the Organization is in compliance with this Standard.</p>
<p>7. <u>Application Management Standard C.1</u>: Is there a control that ensures that user needs result in appropriate program change requests and the requests are properly developed?</p>	<p>See row 2 above. (Standard 13)</p>	<p>See row 2 above. (Standard 13)</p>	<p>The Examiners determined the Organization is in compliance with the Standard.</p>
<p>8. <u>Application Management Standard C.3</u>: Is appropriate program, system, and parallel (when possible) testing performed by the IS staff and QA/User staff to prevent or detect errors in program coding and to ensure that the</p>	<p>See row 2 above. (Standard 13)</p>	<p>See row 2 above. (Standard 13)</p>	<p>The Examiners determined the Organization is in compliance with the Standard.</p>

Standard	Observation from Prior Examination	Organization's Response and Actions	Current Examination Follow-Up
<p>application operates as intended in the production environment and provides accurate data output?</p>			
<p>9. <u>Application Management Standard C.6</u>: Is there a control that ensures that only properly tested, reviewed, and approved changes are transferred into the production environment?</p>	<p>See row 2 above. (Standard 13)</p>	<p>See row 2 above. (Standard 13)</p>	<p>The Examiners determined the Organization is in compliance with the Standard.</p>
<p>10. <u>Operations and Processing Controls Standard E.10</u>:</p> <p>a) Is there a procedure for independent testing and validation of system changes or corrections?</p> <p>b) Is there a procedure for independent testing and validation of the accuracy and completeness of data used in ratemaking or in statistical reports? Please provide a copy of the procedures and evidence of compliance with the procedures for the last change, correction, ratemaking, or statistical report cycle.</p>	<p>The Examiners confirmed that changes to the statistical reporting applications are tracked in a Lotus Notes database and an internally developed migration tool named Integration Test is utilized. However; there was no evidence of change testing and migration approval is not maintained.</p>	<p>See row 2 above. (Standard 13)</p>	<p>The Examiners determined the Organization is in compliance with the Standard.</p>

VI. REVIEW OF EXAMINATION STANDARDS

This aspect of work provides expanded details regarding the Examiners' findings from the prior examination as well as an update for each applicable Standard reviewed during the Examination. Chapter 25 of the NAIC Market Regulation Handbook includes the Standards reviewed, which also included reference to Appendix F. Finally, the Examiners investigated the request by the California Department of Insurance regarding certain of ISS' processes.

ISS is a wholly owned subsidiary of PCI. PCI provides the Organization with operational support such as information technology, legal, etc. Consequently, with ISS' cooperation, the Examiners met with representatives of PCI during the Examination.

The overall results of the targeted Examination did not identify any systemic issues or significant matters concerning ISS' operations.

A. Chapter 25 - Operations/Management/Governance Standards

<p>Standard 12: <i>The advisory organization has an up-to-date, valid internal or external audit program.</i></p>
--

Subsequent Event from Prior Examination: Following conclusion of the prior Examination, the Organization advised the EIC that ISS has undertaken the following remediation efforts with regard to the findings for Standard 12 as follows:

“The ISS board, at its July 14, 2013 meeting, implemented an external audit program to include an audit of financials, IT and statistical reporting under the oversight of the Audit Committee. At its July 15, 2013 meeting, the Audit Committee approved the program and the inclusion of ISS as a standing agenda item for each meeting to ensure regular consideration.”

Results from Current Examination: The Examiners obtained a listing of all audits performed by the Organization during the Period and selected a sample of three audits to review: the MIS audit performed in 2015; the Licensing audit performed in 2016; and the MIS audit performed in 2017. The Examiners also reviewed a written description of the audit process and conducted an onsite discussion with members of the Organization about the process subsequent to the review of the

description. Based on the review performed, the Examiners concluded that ISS does have a valid audit program. However, the Examiners have recommendations for improvement.

Observations: The Examiners met with members of ISS on July 30, 2018. In preparation for the meeting, the IT Examiner requested a sample of Internal Audit reports for the Period. Hard copies of the reports were provided for review of Internal Audit's documentation. In addition, the Examiners reviewed the supporting workpapers within the Organization's documentation repository. The Examiners determined the following from the review of the internal audit information:

- The scope of the work performed appears to be appropriate
- The sampling procedures used were not adequately defined nor documented
- Test plans are not adequately designed to test the controls.
- Tests are executed in accordance with the Test Plans.
- The work was properly documented
- The conclusions reached by the Organization were consistent with the results of the work performed.

Recommendation: ISS should continue to focus on enhancing their Internal Audit testing procedures and documentation. The Internal Audit reports should include sampling procedures which were utilized, and which should include details for determining and validating the populations. In order to place reliance on Internal Audit's work, the populations being tested must be complete and accurate. In addition, in order to test management's review of user access, Internal Audit should begin with a review of the supporting management documentation to determine that user access listings are complete and accurate, and that segregation of duties was maintained (i.e. management isn't reviewing their own access). Once the integrity of management's review has been determined, Internal Audit should then select a random sample of user access reviews to determine the following:

- The access for the user is appropriate based on the job function
- Any changes/updates to the access have been performed.

Finally, the audit report should include the Internal Auditor's opinion (Effective, Satisfactory, Needs Improvement, etc.) regarding the controls tested with a definition of resulting ratings. Additionally, the

audit report should include confirmation that the audit findings have been reviewed with the process owner including documentation of applicable remediation recommendations.

Standard 13: *The advisory organization has appropriate controls, safeguards and procedures for protecting the integrity of computer information.*

Subsequent Event from Prior Examination: Following the conclusion of the prior Examination, the Organization advised the EIC that ISS has undertaken the following remediation efforts with regard to the findings for Standard 13 as follows:

Change Testing Evidence

ISS has expanded its user acceptance testing process to include the retention of the test results that was the basis for user approval. Test results will vary by the scope and complexity of the project and could include screen, report and/or data samples.

ISS implemented the retention of the test results on July 1, 2013.

Application Migration Approval

ISS has expanded its migration process to include management review of recently completed migrations to ensure that the migration approval has been documented in the Change Management System.

*ISS implemented the review on July 1, 2013.**

Results from Current Examination: The IT Examiners reviewed the Organization's Internal Audit reports from the Period and noted the following comments regarding the scope of audits related to ISS' change management process: "The scope of this review is to confirm that changes to the business application are initiated, reviewed and approved by the requesting business area. Additionally, the review confirms change management practices are in place that require authorization and documentation of the migration for business-approved changes, from the test to production environment. The executed change management process and the details of the migration were documented. Supporting documentation was included for each change consisting of test results, reports, and screen prints of the change's progress and final results."

To validate the results of the Internal Audit reports, the IT Examiner selected samples of change requests, which included simple, complex, and emergency changes. The IT Examiner confirmed that when a change is initiated there is a different ISS and/or PCI resource responsible to approve the changes. The IT Examiners also confirmed approved changes are tested prior to the change moving to the production phase. Therefore, based on the Examiner's review and testing, the Organization was determined to be in compliance with the Standard.

Observations and Recommendations: None

Standard 17: *The advisory organization is appropriately licensed.*

Recommendation from Prior Examination: The Examiners recommended that ISS undertake a review of their current processes related to being licensed as an advisory organization and institute revisions to those processes to ensure the Organization can confirm and demonstrate they have the appropriate authority in place for each jurisdiction in which they conduct business. In response, ISS has confirmed the Organization has reviewed its current process and has added a process to contact States that do not acknowledge licensing or confirm receipt of reports.

Results from Current Examination: The Examiners requested information from ISS to confirm their authority to operate in each jurisdiction in which they conduct business, which includes all 50 states, the District of Columbia, and Puerto Rico. The Examiners reviewed documentation and related information provided by ISS, which included the Organization's description of the process for calendar year 2017 and screenshots of the Organization's tracking spreadsheet, which is newly implemented since the prior examination.

Subsequent to reviewing the Organization's licenses and/or registrations for each jurisdiction in which the Organization operates and reviewing the Organization's license renewal and update procedures, the Examiners conducted an onsite discussion with members of ISS.

The following are newly implemented steps by ISS to ensure compliance to Standard 17:

- Generation of Monthly License Status Reports
- Confirmation of DOI contact
- Generation of License Renewal
- Confirmation of License Renewal

- Documentation in the Tracking Spreadsheet and on the System

The Examiners determined ISS satisfies the requirements of Standard 17 based on discussions with ISS and PCI, and the review of supporting documentation including the newly implemented process to ensure the Organization maintains accurate licensing.

Observations and Recommendations: None

B. Appendix F of Chapter 25 - Management and Organizational Controls

The IT Examiners' workplan included procedural reviews, including process walkthroughs with representatives of ISS familiar with the functional aspects of the relevant areas, as well as performing testing to address the areas of Appendix F as follows:

i. Logical and Physical Security

The purpose of this aspect of the Examination was to review issues associated with the Organization's Physical Security systems, processes, procedures, and protocols, which included the following Standards from Appendix F:

B6. Does user department management periodically validate the access capabilities provided to individuals in the department? Please provide evidence of the last user access review performed during the period under review.

And

B14. Are periodic checks carried out to confirm that employees' current application access is commensurate with job responsibilities?

Subsequent Event from Prior Examination: Following conclusion of the prior Examination, the Organization advised the EIC that ISS has undertaken the following remediation efforts with regard to the findings for Standards B6 and B14 in Appendix F and Standard 12 of Chapter 25 as follows:

"ISS has expanded its security management process for the mainframe environment and the statistical reporting system to address the issues of periodic review and documentation.

Mainframe Environment

For the mainframe environment, ISS is implementing a process for management review of user access across the LPARs (test and production) that will include:

- *Distribution of access rights for each active person, by the security administrator, to the appropriate department manager*
- *Review and signoff of the access rights for each person by department manager*
- *Retention of the signoff in the security repository*

ISS will complete this assessment annually in January, to align with the assignment planning process. This process will be completed during the 2nd half of 2013, with implementation January 1, 2014.

Statistical Reporting Systems

For the statistical reporting system, ISS is revising its security administration application to retain the appropriate documentation of the annual review currently done for active staff. This process will result in the following:

- *Retention of the planned assignments for the new year*
- *Online modification of individual access rights based upon project assignments by the appropriate project manager(s)*
- *Online review and signoff of all access rights for each person by the department manager, based upon the planned assignments for the year*
- *Online access to the history of annual changes and department management signoff*

ISS will complete this assessment annually in January, to align with the assignment planning process. Development and testing of the new online signoff process will be completed during the 2nd half of 2013, with implementation January 1, 2014.”

Results from Current Examination: The Examiners determined, based on the work conducted, that ISS has an adequate access review process. However, in order to access the ISS mainframe, users must first authenticate to the Active Directory managed by PCI. Based on the IT Examiners' procedures, it was determined that PCI does not review user accounts on a periodic basis; therefore, the Organization is not in compliance with the Standard. In addition, the IT Examiners noted that PCI does not periodically review the access listings for the doors and IT rooms.

Observations: Based on the IT examination procedures, it was determined that PCI does not review user accounts on a periodic basis. In addition, there is no formal review of the access listings for the floors.

Recommendation: PCI maintains the Active Directory, which the Organization requires for authenticating to the network. As such, ISS should share the results of this Examination with PCI who in turn should perform a review of user access on an annual basis in conjunction with the ISS user access review. In addition, the physical access listings for the office/floors/IT closets should also be reviewed on an annual basis.

B19. If wireless technologies are deployed, does the company monitor for rogue access points.

Subsequent Event from Prior Examination: Following conclusion of the prior Examination, the Organization advised the EIC they have undertaken the following remediation efforts as follows:

“PCI security staff is performing monthly scans of the headquarters facilities to identify any rogue access points that may be attached to the PCI network. This was implemented on 5/6/2013 and added to the IT Security Policy Document.”

Results from Current Examination: The IT Examiners identified that monitoring of the network (firewalls, wireless access points, etc.) is managed by PCI and under agreement with IBM.

The IT Examiners determined the Organization is in compliance with Appendix F – B19 based on discussions with ISS and PCI and through the review of supporting documentation.

Observations and Recommendations: None

ii. Application Management

The purpose of this aspect of the Examination is for the Examiners to review matters associated with the Appendix F - Organization’s Application Management Process, Procedures and Protocols.

C1. Is there a control that ensures that user needs result in appropriate program change requests and the requests are properly developed?

And

C3. Is appropriate program, system and parallel (when possible) testing performed by the IS staff and QA/User staff to prevent or detect errors in program coding and ensure that the application operates as intended in the production environment and provides accurate data output?

And

C6. Is there a control that ensures that only properly tested, reviewed and approved changes are transferred into the production environment?

Subsequent Event from Prior Examination: Following conclusion of the prior Examination, the Organization advised the EIC that ISS has undertaken the following remediation efforts with regard to the findings for Standards 13, C1, C3, and C6. Reference is made to the Organization's details included under Subsequent Event for Standard 13.

Results from Current Examination: The IT Examiners reviewed the Organization's Internal Audit reports from the Period and noted the following comments regarding the scope of audits related to ISS' changes to their business application process. "The scope of this review is to confirm that changes to the business application are initiated, reviewed and approved by the requesting business area. Additionally, the review confirms change management practices are in place that require authorization and documentation of the migration for business-approved changes, from the test to production environment. The change management process was executed and the details of the migration were documented. Supporting documentation was included for each change consisting of test results, reports, and screen prints of the change's progress and result." The IT Examiners selected additional change samples, which included simple, complex, and emergency changes. The IT Examiners reviewed the change documentation and confirmed that the changes were requested and approved by different personnel, the changes were approved after they were requested and that the changes were tested prior to moving into production.

The IT Examiners determined ISS is in compliance with Appendix F – C1, C3 and C6, based on discussions with ISS and PCI and through the review of supporting documentation.

Observations and Recommendations: None

iii. Operations and Processing Controls

The purpose of this aspect of the Examination is for the Examiners to review matters associated with the Organization's Operations and Processing Controls.

E10. a) Is there a procedure for independent testing and validation of system changes or corrections?

b) Is there a procedure for independent testing and validation of the accuracy and completeness of data used in ratemaking or in statistical reports? Please provide a copy of the procedures and evidence of compliance with the procedures for the last change, correction, ratemaking or statistical report cycle.

Subsequent Event from Prior Examination: Following conclusion of the prior Examination, the Organization advised the EIC that ISS has undertaken the following remediation efforts with regard to the findings for E10 a) and b). Reference is made to the Organization's details included under Subsequent Event for Standard 13.

Results from Current Examination: ISS has developed the Submission Processing application (the "Application") which provides companies with a way to upload, validate, edit, and submit their statistical reporting submissions. The Application is a mainframe-based application accessed through ISS' proprietary website, and allows statistical data to be submitted, validated, corrected, and approved through a Web browser. The Application streamlines the data submission process, provides consistent validation, and provides more visibility and control for ISS' affiliates of their data – including the ability to make corrections directly online.

ISS' data validation process (the "Process") further improves the quality of data used in the production of ratings. The Process begins when the front-end editing is complete. Validation tests are run against the database with specific parameters to look for patterns and anomalies within the aggregate data, such as Row/Parsing errors and Business Logic errors. Company

Distribution Analysis is the procedure by which statistically submitted data is compared to financially reported data. Data is reconciled to each accounting year and compared by state, annual statement line, and type of statistic. Subscribers that report statistical data to ISS are required to reconcile their data on an annual basis. ISS compares (by state, annual statement line, and type of statistic) each Subscriber's calendar year statistically reported data to the NAIC as part of each group's annual statement.

The Examiners determined the Organization is in compliance with Standards E10a) and b) as confirmed through the review of samples of the processes described above, and confirmation that the data validation and completeness tests were performed by ISS and PCI.

Observations and Recommendations: None

C. REVIEW OF STATISTICAL PLANS

There were no findings identified during the prior examination regarding statistical plans, and therefore this area was excluded from the scope of the current Examination. However, the Examiners did conduct a discussion with ISS focused on any potential changes made to the statistical plans during the Period. ISS provided a general overview regarding the staffing, communication, and processes related to the statistical plans. The Organization advised the Examiners that the data validation and data summary processes have not changed since the prior Examination. Relevant changes that did occur during the Period included a new NAIC analysis screen, which captures changes on an annual basis, and additions and/or changes to class codes, lines of business, and territories. No areas of concerns were identified.

D. REPORTS, REPORT SYSTEMS, AND OTHER DATA REQUESTS

The Data Collection and Handling process Standard was not included in the scope of the Examination. However, at the request of the California Department of Insurance, which is a Participating State for the Examination, the Examiners did perform limited procedures to review the Organization's processes regarding production of Fast Track data and Experience Data listings.

In response to the request, the Examiners performed the following procedures:

- Walkthrough of the Fast Track and Experience Data processes.
- Select a sample submission and track the submission through the data process to the final report.

The Examiners reviewed information submitted by two California Subscribers during the course of the walkthrough. In confirming that the Organization adequately reviews statistical data collected for quality and compiled according to applicable statutes, rules, and regulations, the Examiners met with ISS and PCI resources who have direct access to the data and who could reconcile various values from the Experience Data and Fast Track data in the relevant databases. The Examiners performed the following:

- Reviewed the Data Control screen, which shows the progress of the Data Call for 2017: The Examiners confirmed that the Data Control screen is used by ISS to monitor the status of the Data Call and determine if there are any outstanding submissions. The Examiners reviewed the Subscriber's submission writing premium in California (the name was redacted) and confirmed "Zero error records were found for this submission," which indicates that the initial process to identify errors in the data was performed.
- Confirmed the applicable data submissions were subject to the editing process: The Examiners noted that the Balance Status of the submission for a different Subscriber who writes premium in California was "B," which indicates that the editing process was completed without any errors.
- Confirmed the applicable data was moved from the Data Submission application into the Data Summary (i.e. data warehouse) by confirming the Date Received Timestamp.
- Confirmed data completeness tests were performed by ISS: The Examiners noted that the Submission Status was a "1," which indicates that the submission had been reviewed and approved by ISS personnel

The Examiners also discussed ISS' process related to ensuring that statistical data received by ISS is reconciled to the information provided on the NAIC Annual Statement, confirming the integrity of the information in the Fast Track Monitoring report. The Examiners selected two values for review from the Fast Track Monitoring report as follows:

- Earned Premium - The Examiners noted that the Earned Premium for California was \$940,019,572 as shown on the State Distribution Analysis. That value matched the value on

the Fast Track Monitoring report for California Q1 2018. The Examiners reviewed the Company Distribution Analysis, which reflected a total of \$940,019,572.

- Incurred Losses - The Examiners noted that the Incurred Losses for California was \$208,318,924 as shown on the State Distribution Analysis. That value matched the value on the Fast Track Monitoring report for California Q1 2018. The Market Conduct Examiners reviewed the Company Distribution Analysis, which reflected a total of \$208,318,924.

Based on the review of the documents, the Examiners concluded information is accurately maintained in the Organization's systems and is correctly used to populate the Fast Track Monitoring and Experience Data reports. In addition, the Examiners determined that the information reconciles to the annual NAIC reporting.

VII. Examination Summary

Standard	Observations and Recommendations
<p><u>1. Operations/Management/ Governance Standard 12:</u> The advisory organization has an up-to-date, valid internal or external audit program.</p>	<p>The Examiners determined the following from the review of the internal audit information:</p> <ul style="list-style-type: none"> • The scope of the work performed appears to be appropriate. • The sampling procedures used were not adequately defined nor documented. • Test plans are not adequately designed to test the controls. • Tests are executed in accordance with the Test Plans. • The work was properly documented. • The conclusions reached by the Organization were consistent with the results of the work performed. <p>ISS should continue to focus on enhancing their Internal Audit testing procedures and documentation. The Internal Audit reports should include the sampling procedures which were utilized and should include details for determining and validating the populations. In order to place reliance on Internal Audit's work, the populations being tested must be complete and accurate. In addition, in order to test management's review of user access, Internal Audit should begin with a review of the supporting management documentation to determine that user access listings are complete and accurate and that segregation of duties was maintained (i.e. management isn't reviewing their own access). Once the integrity of management's review has been determined, Internal Audit should then select a random sample of user access reviews to determine the following:</p> <ul style="list-style-type: none"> • The access for the user is appropriate based on the job function • Any changes/updates to the access have been performed. <p>Finally, the audit report should include the Internal Auditor's opinion (Effective, Satisfactory, Needs Improvement, etc.) regarding the controls tested with a definition of resulting ratings. Additionally, the audit report should include confirmation that the audit findings have been reviewed with the process owner including documentation of applicable remediation recommendations.</p>
<p><u>2. Operations/Management/ Governance Standard 13:</u> The advisory organization has appropriate controls, safeguards</p>	<p>The Organization is in compliance with the Standard.</p>

Standard	Observations and Recommendations
and procedures for protecting the integrity of computer information.	
<u>3. Operations/Management/ Governance Standard 17:</u> The advisory organization is appropriately licensed.	The Organization is in compliance with the Standard.
<u>4. Logical and Physical Security Standard B.6:</u> Does user department management periodically validate the access capabilities provided to individuals in the department? Please provide evidence of the last user access review performed during the period under review.	<p>ISS has an adequate access review process. However, in order to access the ISS mainframe, the users must first authenticate to the Active Directory managed by PCI. Based on the examination procedures, it was determined that PCI does not review user accounts or physical access listings on a periodic basis; therefore, the Organization <i>does not comply</i> with the Standard.</p> <p>Recommendation: Since PCI maintains the Active Directory which ISS requires for authenticating to the network, PCI should perform a review of user access on an annual basis in conjunction with the ISS user access review. In addition, the physical access listings for the office/floors/IT closets should be reviewed on a periodic basis.</p>
<u>5. Logical and Physical Security Standard B.14:</u> Are periodic checks carried out to confirm that employees' current application access is commensurate with job responsibilities?	This Standard is linked with Standard B.6. The Organization does not comply with this Standard.
<u>6. Logical and Physical Security Standard B.19:</u> If wireless technologies are deployed, does the company monitor for rogue access points.	The Organization is in compliance with the Standard.
<u>7. Application Management Standard C.1:</u> Is there a control that ensures that user needs result in appropriate program change requests and the requests	The Organization is in compliance with the Standard.

Standard	Observations and Recommendations
are properly developed?	
<p><u>8. Application Management Standard C.3:</u> Is appropriate program, system and parallel (when possible) testing performed by the IS staff and QA/User staff to prevent or detect errors in program coding and ensure that the application operates as intended in the production environment and provides accurate data output?</p>	<p>The Organization is in compliance with the Standard.</p>
<p><u>9. Application Management Standard C.6:</u> Is there a control that ensures that only properly tested, reviewed and approved changes are transferred into the production environment?</p>	<p>The Organization is in compliance with the Standard.</p>
<p><u>10. Operations and Processing Controls Standard E.10:</u></p> <p>a) Is there a procedure for independent testing and validation of system changes or corrections?</p> <p>b) Is there a procedure for independent testing and validation of the accuracy and completeness of data used in ratemaking or in statistical reports? Please provide a copy of the procedures and evidence of compliance with the procedures for the last change, correction,</p>	<p>The Organization is in compliance with the Standard.</p>

Standard	Observations and Recommendations
ratemaking or statistical report cycle.	

VIII. Examination Report Submission

We acknowledge the courtesy and cooperation of the officers and employees of the Organization during the Examination.

Respectfully submitted,



Barry L. Wells, CCLA, AMCM
Risk and Regulatory Consulting, LLC
Examiner-in-Charge