Attachment 1

Draft: 1/14/19

Market Conduct Examination Standards (D) Working Group
Conference Call
December 19, 2018

The Market Conduct Examination Standards (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met via conference call Dec. 19, 2018. The following Working Group members participated: Bruce R. Ramge, Chair, Laura Arp and Reva Vandevoorde (NE); Jim Mealer, Vice Chair, and Cynthia Amann (MO); Melissa Grisham and Mel Heaps (AR); Adam Boggess, Bruce Glaser and Damion Hughes (CO); Stephen Deangelis and Kurt Swan (CT); Kay Godfredson (IA); Lori Cunningham and Russell Hamblen (KY); Mary Lou Moran (MA); Melinda Domzalski-Hansen, Paul Hanson and Alley Zoellner (MN); Maureen Belanger, Jennifer Patterson and Win Pugsley (NH); Ralph Boeckman and Chanell McDevitt (NJ); Peggy Willard-Ross (NV); Sylvia Lawson (NY); Rodney Beetch and Angela Dingus (OH); Katie Dzurec and Kelly Krakowski (PA); Julie Blauvelt and Yolanda Tennyson (VA); John Haworth and Jeanette Plitt (WA); Sue Ezalarab and Rebecca Rebholz (WI); and Barbara Hudson (WV).

1. Adopted its Nov. 29 Minutes

The Working Group met Nov. 29 and took the following action: 1) discussed new mental health parity-related guidance for inclusion in the *Market Regulation Handbook* (Handbook); 2) discussed new insurance data security pre- and post-breach checklists; and 3) discussed new standardized data requests for private passenger auto in-force policies, private passenger auto claims and personal lines declinations.

Ms. Plitt made a motion, seconded by Mr. Pugsley, to adopt the Working Group's Nov. 29 minutes (Attachment XXX). The motion passed unanimously.

2. Adopted New Mental Health Parity-Related Guidance for inclusion in the Handbook

Director Ramge said that the two mental health parity-related exposure drafts before the Working Group consist of: 1) a general guidance document addressing mental health parity review, which includes a series of questions to be posed to health carriers by examiners, to be inserted in a chapter or area to be determined of the Handbook; and 2) a state insurance regulator data collection tool for mental health parity analysis. He said the drafts, which were developed with the assistance of regulator subject matter experts (SMEs) in mental health parity review, were circulated on July 9; they were initially discussed during the Working Group's July 25 conference call and subsequently during its Aug. 29 and Nov. 29 calls. Ms. Arp revised the two draft documents on Dec. 11, taking into consideration suggestions received from Maryland, the Association for Behavioral Health and Wellness (ABHW), and joint comments received from the NAIC consumer representatives.

Pamela Greenberg (ABHW) presented comments dated Dec. 5 and provided comments on the Dec. 11 exposure drafts. Ms. Greenberg asked that the Working Group consider adding a new question to the general guidance document: "Are all conditions that are defined as being or as not being a mental health condition, a substance use disorder or a medical condition defined in a manner that is consistent with generally recognized independent standards of current medical practice?" Ms. Arp made a motion, seconded by Mr. Mealer, to make this change to the document. Ms. Greenberg also suggested that the word "methodology" be used instead of "factors" in Question 4 and Question 5 in the general guidance document. Mr. Mealer made a motion, seconded by Ms. Plitt, to make this change.

Ms. Greenberg said she supports the addition of the federal Centers for Medicare & Medicaid Services (CMS) Table 5 in the non-quantitative treatment limitations (NQTL) data collection tool exposure draft. She suggested that a note be added to the NQTL table, in the explanation column, indicating that the regulated entity being examined explain how mental health/substance use disorder benefits compare to medical surgical benefits. Ms. Arp made a motion, seconded by Ms. Rebholz, to make the revision to the document.

Mr. Mealer made a motion, seconded by Ms. Dingus, to adopt both mental health parity exposure drafts to include all changes made during the conference call (Attachment XXX and Attachment XXX). The motion passed unanimously.

3. Reviewed Insurance Data Security Pre- and Post-Breach Checklists, Dec. 17 Draft

Director Ramge said the Insurance Data Security Pre- and Post-Breach Checklists, which were first distributed on July 16, 2018, were developed to correlate with the *Insurance Data Security Model Law* (#668), which was adopted by the Executive (EX) Committee and Plenary on Oct. 24, 2017. The checklists, developed by regulator SMEs in the fields of market examinations and financial examinations, provide examiners with guidance on evaluating the insurance data security of regulated entities. Director Ramge said that the draft checklists were initially discussed during the Working Group's July 25, Aug. 29 and Nov. 29 conference calls, and a revised draft was distributed on Dec. 17, 2018.

Director Ramge said the Dec. 17 draft incorporates language that had been adopted by the IT Examination (E) Working Group in October to address issues regarding collaboration and the states' adoption of the model, to date, raised by interested parties. Director Ramge said the difference between the exposure draft previously circulated and the Dec. 17 draft is the incorporation of the language "or legislation which is substantially similar to the model" so that the language then reads: "Note: The guidance that follows should only be used in states that have enacted the NAIC *Insurance Data Security Model Law* (#668) or legislation which is substantially similar to the model. Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department including but not limited to financial examination-related work."

Robyn Anderson (Old Republic National Title Insurance Company) presented comments dated Dec. 13. She said that pre-breach examiner review should be performed by financial examiners in the information technology (IT)-related portion of a financial examination. Ms. Anderson said that the requirements set forth in the pre- and post-breach checklists differ substantially from the model, and thus could raise confusion and impose additional requirements beyond those set forth in the model. Ms. Anderson asked that the Working Group discard the pre-breach checklist and retain the post-breach checklist.

Angela Gleason (American Insurance Association—AIA) presented comments dated Dec. 17. She expressed concerns about the efficiency, scope, duplication and coordination of pre-breach market examiner review and pre-breach financial examiner review. Ms. Anderson said that placement of the pre-breach checklist in the Handbook reference documents does not lead to uniformity and that the correct placement of pre-breach review is in financial-related examinations.

Robbie Meyer (American Council of Life Insurers—ACLI) presented comments dated Dec. 18. She asked that the Working Group not consider inclusion of the pre-breach checklist in the Handbook for use as part of a market conduct exam. Ms. Meyer suggested that the best place for pre-breach review is in the context of a financial examination. Ms. Meyer added that if the Working Group retains the pre-breach checklist, the criteria in the pre-breach checklist, as well as the post-breach checklist, should be revised so that it tracks more closely to the model.

Ms. Plitt said that the pre-breach checklist would be a valuable tool for examiners, should a pre-breach review be deemed necessary, in the course of a market conduct examination; she therefore asked that the pre-breach checklist be retained in the Handbook. Director Ramge said that it had been previously suggested during the Working Group's Nov. 29 conference call that the pre-breach checklist be incorporated into the reference documents of the Handbook in order to make the resource readily available to market conduct examiners, while not incorporating the checklist directly into the Handbook.

Director Ramge asked the Working Group to decide: 1) whether to proceed with the review of the pre-breach checklist exposure draft, with the inclusion of language to be developed by NAIC staff, that market regulators coordinate with domestic financial regulators; or 2) whether to remove the pre-breach checklist, in its entirety, from the Working Group's review.

Ms. Plitt made a motion, seconded by Mr. Mealer, that the Working Group proceed with the review of the pre-breach checklist exposure draft, with the inclusion of language to be developed by NAIC staff, that market regulators coordinate with domestic financial regulators, and to also consider making technical changes outlined in the comments received from the ACLI (Attachment XXX). The motion passed unanimously.

Director Ramge asked that comments be submitted on the pre- and post-breach checklists by Dec. 31.

4. <u>Reviewed New Standardized Data Requests for Inclusion in the Reference Documents of the Handbook</u>

Director Ramge said that two new private passenger auto standardized data requests and a personal lines declination standardized data request had been developed by regulator SMEs for the Working Group's review, discussion and adoption. When the standardized data requests are adopted, they will replace the private passenger auto portion of the NAIC personal lines standardized data request.

Birny Birnbaum (Center for Economic Justice—CEJ) said that when examiners review regulated entity claim settlement practices, the review of additional fields not listed in the claims standardized data request (e.g., rating factors) may be necessary. Mr. Hamblen said that the intent of the standardized data requests is not to provide an all-encompassing listing of all fields that could be reviewed in examination; rather, the standardized data requests are a listing of most commonly used fields in a typical review of regulated entity market conduct practices. Mr. Hamblen said that states are encouraged to use the standardized data requests as a template and to build upon the template; states may remove fields or add fields as necessary, depending on the circumstances, scope and purpose of an examination. Mr. Birnbaum asked that the Working Group consider adding additional fields to the standardized data requests regarding a regulated entity's use of credit scores, price optimization tools and claim automation algorithms.

Director Ramge asked that comments be submitted on the standardized data requests by Dec. 31.

5. Discussed Other Matters

Director Ramge said NAIC staff will provide advance email notice of the next Working Group conference call, which is anticipated to occur early in 2019, after the Working Group is reappointed by the Market Regulation and Consumer Affairs (D) Committee.

Having no further business, the Market Conduct Examination Standards (D) Working Group adjourned.

W:\National Meetings\2019\Spring\Cmte\D\MCES\12-19.docx

Attachment 2

Potential Market Conduct Examination Standards (D) Working Group 2019 Tasks

For the purpose of generating discussion, the following is a list of recently adopted NAIC Models to consider for development of corresponding revisions to the *Market Regulation Handbook* in 2019. This is a preliminary listing of potential tasks which the Working Group may be focusing on in 2019, in addition to the current work being done by the Working Group on the Insurance Data Security Model Pre-Breach and Post-Breach Checklists and Standardized Data Requests. The Working Group's potential tasks in 2019 are not limited to the below, and this listing does not preclude additional tasks which may be added during the year, by the Working Group, or at the request of the Market Regulation and Consumer Affairs (D) Committee.

Model #	**Title of Model**	**Date of adoption**
632	Travel Insurance Model Act	4th Q 2018
642	Limited Long-Term Care Insurance Model Act	4th Q 2018
643	Limited Long-Term Care Insurance Model Regulation	4th Q 2018
	Are there any other models to consider?	

MARKET REGULATION HANDBOOK
INSURANCE DATA SECURITY PRE-BREACH AND POST-BREACH CHECKLISTS

Company Name	
Period of Examination	
Examination Field Date	
Prepared By	
Date	

GUIDANCE

NAIC Insurance Data Security Model Law (#668)

Note: The guidance that follows should only be used in states that have enacted the *NAIC Insurance Data Security Model Law (#668)* or legislation which is substantially similar to the model. Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department including but not limited to financial examination-related work.

OVERVIEW

The purpose and intent of the Insurance Data Security Model Law is to establish standards for data security and standards for the investigation of and notification to the Commissioner or Director of Insurance of a Cybersecurity Event affecting Licensees.

REVIEW GUIDELINES AND INSTRUCTIONS

When reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668) for the prevention of a Cybersecurity Event as defined in the model law, please refer to the examination checklist attached as Exhibit A hereto.

When reviewing a Licensee's Information Security Program and response to a Cybersecurity Event for compliance with the Insurance Data Security Model Law subsequent to a suspected and/or known Cybersecurity Event as defined in the model law, please refer to both examination checklists attached as Exhibits A and Exhibit B hereto.

When considering whether to underake such a review, refer to Section 9 of NAIC Model #668, which provides certain exceptions to compliance for Licensees with fewer than ten employees; Licensees subject to the Health Insurance Portability and Accountability Act (Pub.L, 104-191, 110 Stat. 1936, enacted August 21, 1996); and certain employees, agents, representatives, or designees of Licensees who are in themselves Licensees.

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

INFORMATION SECURITY PROGRAM (Sections 4A and 4B)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
1. Does the Licensee have a written Information Security Program (ISP)?	
2. Does the ISP clearly state the person(s) at the Licensee responsible for the program?	
3. Has the ISP been reviewed and approved by the Licensee’s executive management?	
4. Has the ISP been reviewed and approved by the Licensee’s Board of Directors? (Section 4E)	
5. Has the ISP been reviewed and approved by the Licensee’s IT steering committee?	
6. How often is the ISP reviewed and updated? (Section 4G)	
7. Are any functions of the ISP outsourced to third parties? (*If YES, identify any such providers, review their roles and responsibilities, and the Licensee’s oversight of the third parties*.)	
8. Does the ISP contain appropriate administrative, technical and physical safeguards for the protection of Nonpublic Information and the Licensee’s Information Systems?	
9. Does the Licensee stay informed regarding emerging threats and vulnerabilities? (Section 4D(4))	
10. Does the Licensee regularly communicate with its employees regarding security issues?	
11. Does the Licensee ensure that employees’ hardware is updated on a timely basis to ensure necessary security software updates and patches have been downloaded and installed?	
12. Does the Licensee provide cybersecurity awareness training to its personnel? (Section 4D(5))	
13. How soon after onboarding a new employee does the Licensee provide cybersecurity awareness training? At what intervals is the training renewed?	
14. Does the Licensee utilize reasonable security measures when sharing information? (Section 4D(4))	

Exhibit A: **Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17**
Insurance Data Security Model Law #668, Section 4

RISK ASSESSMENT (Section 4C)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
15. Has the Licensee conducted a Risk Assessment to identify foreseeable internal and external threats to its information security?	
16. When was the last Risk Assessment conducted or updated?	
17. Has the Licensee designed its ISP to address issues identified in its Risk Assessment?	
18. Are Cybersecurity Risks included in the Licensee's Enterprise Risk Management process? (Section 4D(3))	

COMPONENTS OF INFORMATION SECURITY PROGRAM (Section 4D)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
19. Has the Licensee determined that the following security measures are appropriate, and has the Licensee implemented them as part of its ISP? *(If NO for any item, interview the appropriate responsible personnel to discuss the reason(s) such measures were not implemented.)*	
19a. Access controls to limit access to Information Systems to Authorized Individuals?	
19b. Physical controls on access to Nonpublic Information to limit access to Authorized Individuals?	
19c. Protection of Nonpublic Information by encryption or other appropriate means while being transmitted externally or stored on portable computing devices or media?	
19d. Secure development practices for in-house applications and procedures for testing the security of externally developed applications?	
19e. Controls for individuals accessing Nonpublic Information such as Multi-Factor Authentication?	
19f. Regular testing and monitoring of systems to detect actual and attempted attacks or intrusions into Information Systems?	
19g. Audit trails in the ISP to detect and respond to Cybersecurity Events and permit reconstruction of material financial transactions?	
19h. Measures to prevent Nonpublic Information from physical damage, loss or destruction?	
19i. Secure disposal procedures for Nonpublic Information?	

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

THIRD-PARTY SERVICE PROVIDERS (Section 4F)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
20. Does the Licensee have Third-Party Service Providers with which it shares Nonpublic Information?	
21. Does the Licensee include information security standards as part of its contracts with such providers?	
22. Does the Licensee conduct inspections or reviews of its providers' information security practices?	

INCIDENT RESPONSE PLAN (Section 4H)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
23. Does the ISP contain a written incident response plan and/or detailed process for responding to a Cybersecurity Event?	
24. Does the incident response plan provide clear guidance on when to initiate a Cybersecurity Event investigation?	
25. Does the incident response plan contain a list of clear and well-defined objectives?	
26. Does the incident response plan provide clear roles, responsibilities and levels of decision-making authority?	
27. Does the incident response plan require written assessment of the nature and scope of a Cybersecurity Event?	
28. Does the incident response plan require determination of whether any Nonpublic Information was exposed during a Cybersecurity Event and to what extent?	
29. Does the incident response plan provide clear steps to be taken to restore the security of any information systems compromised in a Cybersecurity Event?	
30. Does the incident response plan sufficiently address steps to take when a Cybersecurity Event occurs at a Third-Party Service Provider where data provided by the Licensee is potentially at risk?	
31. Does the incident response plan provide detailed instructions for external and internal communications, as well as information sharing with regulatory authorities?	
32. Does the incident response plan define various levels of remediation based on the severity of identified weaknesses?	

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

DOCUMENTATION AND REPORTING

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
33. Does the ISP describe documentation and reporting procedures for Cybersecurity Events and related incident response activities? (Section 4H)	
34. Does the ISP require a post-event evaluation following a Cybersecurity Event? (Section 4H)	
35. Does the ISP require retention of all records related to Cybersecurity Events for a minimum of five years? (Section 5D)	
36. Has the Licensee prepared and submitted annual certifications to its domiciliary state Commissioner/Director of Insurance? (Section 4I)	

PRIOR EXAMINATION FINDINGS

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
37. Has the Licensee addressed and implemented corrective actions to any material findings from any prior examinations?	

Exhibit B: Supplemental Incident Response Plan Investigation (Post-Breach) and Notification Cybersecurity Event Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 5 and 6

POST-EVENT INVESTIGATION BY LICENSEE (Section 5)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
1. Did the Licensee conduct a prompt investigation of the Cybersecurity Event? (Section 5A)	
2. Did the Licensee appropriately determine the nature and scope of the Cybersecurity Event? (Section 5B)	

NOTICE TO COMMISSIONER/DIRECTOR OF INSURANCE (Section 6)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
3. Did the Licensee provide timely notice (no later than 72 hours) to the Commissioner or Director of Insurance following the Cybersecurity Event? (Section 6A)	
4. Did the Notification to the Commissioner or Director of Insurance include the following information, to the extent reasonably available? (Section 6B)	
4a. The date of the Cybersecurity Event, or the date upon which it was discovered?	
4b. A description of how the Nonpublic Information was exposed, lost, stolen or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any?	
4c. How the Cybersecurity Event was discovered?	
4d. Whether any lost, stolen or breached Nonpublic Information has been recovered, and if so, how this was done?	
4e. The identity of the source of the Cybersecurity Event?	
4f. Whether the Licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies? *(If YES, did the Licensee provide the date(s) of such notification(s)?)*	
4g. A description of the specific types of Nonpublic Information acquired without authorization?	
4h. The period during which the Information System was compromised by the Cybersecurity Event?	
4i. A best estimate of the number of total Consumers in this state and globally affected by the Cybersecurity Event?	
4j. The results of any internal review of automated controls and internal procedures and whether or not such controls and procedures were followed?	
4k. A description of efforts being undertaken to remediate the circumstances which permitted the Cybersecurity Event to occur?	
4l. A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate the Cybersecurity Event and to notify affected Consumers?	
4m. The name of a contact person familiar with the Cybersecurity Event and authorized to act for the Licensee?	
5. Did the Licensee provide timely updates to the initial notification and Questions 4a-4m above? (Section 6B)	

OTHER NOTIFICATIONS (Section 6)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
6. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to Consumers? (*If YES, did the Licensee provide a copy of the notification to the Commissioner(s)/Directors of all affected states?)* (Section 6C)	
7. Did the reinsurer Licensee provide timely and sufficient notice of the Cybersecurity Event to ceding insurers? (Section 6E)	
8. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to independent insurance producers and/or producers of record of affected Consumers? (Section 6F)	

THIRD PARTY SERVICE PROVIDERS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
9. Did the Cybersecurity Event occur at a Third-Party Service Provider? *(If YES, did the Licensee fulfill its obligations to ensure compliance with this law, either directly or by the Third-Party Service Provider?)* (Sections 5C and 6D)	

POST-EVENT ANALYSIS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
10. What changes if any are being considered to the Licensee's ISP as a result of the Cybersecurity Event and the Licensee's response?	

G:\MKTREG\DATA\D Working Groups\D WG 2019 MCES (PCW)\Docs_WG Calls 2019\Ins Data Security\Current Drafts\IDS Pre&PostBreach Checklists Revised 12-17-18.doc

ACLI
Financial Security...for Life.

Emily Micale
Senior Counsel

February 20, 2019
Director Bruce R. Ramge, Chair
Market Conduct Examinations Standards (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Attn: Petra Wallace

Via e-mail: pwallace@naic.org

Re: Insurance Data Security Pre-Breach and Post-Breach Checklists –ACLI REDLINE of Revised 12-17-18 Draft

Dear Director Ramge:

The American Council of Life Insurers (ACLI) advocates on behalf of 280-member companies dedicated to providing products and services that promote consumers' financial and retirement security. 90 million American families depend on our members for life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, dental and vision and other supplemental benefits. ACLI represents member companies in state, federal and international forums for public policy that supports the industry marketplace and the families that rely on life insurers' products for peace of mind. ACLI members represent 95 percent of industry assets in the United States.

ACLI thanks the Market Conduct Examination Standards (D) Working Group (Working Group) for its continuing discussion of the Insurance Data Security Pre-Breach and Post- Breach Checklists (Checklists), proposed to be included in the Market Regulation Handbook (Handbook) and the opportunity to offer these comments, along with a proposed redlined draft to the most recent NAIC (12/17/18) draft of the Checklists.

ACLI appreciates the inclusion of the Note at the beginning of the Checklists that provides that the following guidance should only be used in states that have adopted the NAIC Insurance Data Security Model Law (Model Law) or substantially similar legislation and that it is important examiners obtain an understanding and leverage the work performed by other units of the department.

As discussed in ACLI's December 18, 2018 Comments, and on the NAIC's December 19, 2018 Working Group call, ACLI reiterates it is not the purpose of the Handbook to specify how jurisdictions allocate market and financial regulation staff when conducting an insurance data security exam. At the same time, ACLI respectfully submits that performance of pre-beach assessments solely as part of the financial examinations will further insurers' resiliency, provide for examinations by individuals likely to have more appropriate expertise for assessing insurers' information security systems, promote efficiency and avoid duplication of work and inconsistent application of examination standards. Accordingly, ACLI respectfully urges the Working Group not to recommend inclusion of a pre-breach Checklist in the Handbook for use as part of a market conduct exam.

If the Working Group determines the above is not possible, in line with discussion during the 12/19/18 Working Group call, ACLI urges modification to the current (12/17/18) draft of the Checklists to provide for the Handbook to: (i) incorporate a post-breach checklist only; and (ii) make any pre-breach guidance available in the Handbook reference documents.

If a pre-breach checklist is provided in the Handbook or its reference documents, ACLI urges that it be preceded by a reminder to examiners that the Model Law specifies that its requirements are to be based on a licensee's risk profile and that insurers' data security systems are to be risk-based.

Further, in line with other comments submitted to the Working Group, ACLI is concerned that a number of the criteria in both the pre-breach checklist and the post-breach checklist are not in the Model Law or deviate from the corresponding provisions of the Model Law. Therefore, along with these comments, we respectfully submit an initial redline draft of the NAIC's 12/17/18 draft of the Checklists to most-closely track the language of the Model.

Therefore, ACLI respectfully submits our redline modifications to the criteria included in any pre or post breach checklist included in the Handbook, or any reference documents of the Handbook, with best efforts to track the language of the Model Law to the greatest extent possible.

ACLI appreciates and thanks the Working Group for its consideration of our concerns and would be glad to answer questions relating to any of the above.

Respectfully submitted,

Emily C. Micale

Emily Micale

G:\MKTREG\DATA\D Working Groups\D WG 2019 MCES (PCW)\Docs_WG Calls 2019\Ins Data Security\Comments Received\ACLI 02-20-19 Comments.docx

MARKET REGULATION HANDBOOK
INSURANCE DATA SECURITY PRE-BREACH AND POST-BREACH CHECKLISTS

Company Name	
Period of Examination	
Examination Field Date	
Prepared By	
Date	

GUIDANCE

NAIC Insurance Data Security Model Law (#668)

Note: The guidance that follows should only be used in states that have enacted the *NAIC Insurance Data Security Model Law (#668)* or legislation which is substantially similar to the model. Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department including but not limited to financial examination- related work.

OVERVIEW

The purpose and intent of the Insurance Data Security Model Law is to establish standards for data security and standards for the investigation of and notification to the Commissioner or Director of Insurance of a Cybersecurity Event affecting Licensees.

REVIEW GUIDELINES AND INSTRUCTIONS

When reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668) for the prevention of a Cybersecurity Event as defined in the model law, please refer to the examination checklist attached as Exhibit A hereto.

When reviewing a Licensee's Information Security Program and response to a Cybersecurity Event for compliance with the Insurance Data Security Model Law subsequent to a suspected and/or known Cybersecurity Event as defined in the model law, please refer to both examination checklists attached as Exhibits A and Exhibit B hereto.

When considering whether to undertake such a review, refer to Section 9 of NAIC Model #668, which provides certain exceptions to compliance for Licensees with fewer than ten employees; Licensees subject to the Health Insurance Portability and Accountability Act (Pub.L, 104-191, 110 Stat. 1936, enacted August 21, 1996); and certain employees, agents, representatives, or designees of Licensees who are in themselves Licensees.

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

INFORMATION SECURITY PROGRAM (Sections 4A and 4B)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
1. Does the Licensee have a written Information Security Program (ISP)?	
2. Does the ISP clearly state the person(s) ~~at the Licensee~~ responsible for the program?	Section 4.C.(1)
3. Has the ISP been reviewed ~~and approved~~ by the Licensee's executive management?	Edited language
4. Has the overall status of the ISP been reviewed ~~and approved~~ by the Licensee's Board of	Section 4.E.(2)(a)
~~5. Has the ISP been reviewed and approved by the Licensee's IT steering committee?~~	Remove, as inapplicable
6. ~~How often is the ISP reviewed and updated?~~Has the Licensee monitored, evaluated and adjusted, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external treats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems?	Section 4.G.
7. Does the Licensee Grant Oversight of the ISP by Third-Party Service Provider Arrangements? Does the Licensee designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the ISP? ~~Are any functions of the ISP outsourced to third parties? *(If YES, identify any such providers, review their roles and responsibilities, and the Licensee's oversight of the third parties.)*~~	Section 4.C.(1) See also Criterion 21 & 22, per Section 4.F.
8. Does the ISP contain appropriate administrative, technical and physical safeguards commensurate with the size and complexity of the Licensee and the nature and scope of the Licensee's activities? ~~for the protection of Nonpublic Information and the Licensee's Information Systems?~~	
9. Does the Licensee stay informed regarding emerging threats and vulnerabilities? (Section 4D(4))	
~~10. Does the Licensee regularly communicate with its employees regarding security issues?~~	N/A per the Model See Criteria 12 below.
~~11. Does the Licensee ensure that employees' hardware is updated on a timely basis to ensure necessary security software updates and patches have been downloaded and installed?~~	See Criteria 6, as amended, above.
12. Does the Licensee provide cybersecurity awareness training to its personnel? (Section 4D(5))	
~~13. How soon after onboarding a new employee does the Licensee provide cybersecurity awareness training? At what intervals is the training renewed?~~	N/A, there is no requirement as to the specific intervals at which cyber-awareness training should occur in the Model.
14. Does the Licensee utilize reasonable security measures when sharing information? (Section 4D(4))	

Commented [EM1]: Criteria 3, 4 and 5: The Model Law requires that an Information Security Program be developed, implemented and maintained by the Licensee's Executive Management and reported on annually.
Nowhere in the Model Law is there a requirement that the Board, IT Steering Committee, or Executive Management approve of the Information Security Program. Additionally, there is no
reference in the Model Law to an IT Steering Committee. The Board can delegate some of its
authority to a committee; however, it should not be assumed that such delegation is to an IT Steering
Committee.

As such, we recommend the following amendments to the left:

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

RISK ASSESSMENT (Section 4C)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
15. Has the Licensee conducted a Risk Assessment to identify foreseeable internal and external threats to its information security?	
16. ~~When was the last Risk Assessment conducted or updated~~? Has the Licensee implemented information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assessed the effectiveness of the safeguards' key controls, systems, and procedures?	Section 4.C.(5)
17. Has the Licensee designed its ISP to address issues identified in its Risk Assessment?	
18. Are Cybersecurity Risks included in the Licensee's Enterprise Risk Management process? (Section 4D(3))	

COMPONENTS OF INFORMATION SECURITY PROGRAM (Section 4D)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT***
19. Has the Licensee determined that the following security measures are appropriate, and has the Licensee implemented them as part of its ISP? *(If NO for any item, interview the appropriate responsible personnel to discuss the reason(s) such measures were not implemented.)*	
19a. Access controls to limit access to Information Systems to Authorized Individuals?	
19b. Physical controls on access to Nonpublic Information to limit access to Authorized Individuals?	
19c. Protection of Nonpublic Information by encryption or other appropriate means while being transmitted ~~externally~~ over an external network or stored portable computing devices or media?	Section 4.D.(2)(d)
19d. Secure development practices for in-house applications and procedures for testing the security of externally developed applications?	
19e. Controls for individuals accessing Nonpublic Information such as Multi-Factor Authentication?	
19f. Regular testing and monitoring of systems to detect actual and attempted attacks or intrusions into Information Systems?	
19g. Audit trails in the ISP to detect and respond to Cybersecurity Events and permit reconstruction of material financial transactions?	
19h. Measures to prevent Nonpublic Information from physical damage, loss or destruction?	
19i. Secure disposal procedures for Nonpublic Information?	

Exhibit A:

Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

THIRD-PARTY SERVICE PROVIDERS (Section 4F)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
20. Does the Licensee have Third-Party Service Providers with which it shares Nonpublic Information?	
21. Does the Licensee exercise due diligence in selecting its Third-Party Service Provider? ~~Does the Licensee include information security standards as part of its contracts with such providers?~~	Per Section 4.F.(1)
22. Does the Licensee require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider?~~. Does the Licensee conduct inspections or reviews of its providers' information security practices?~~	Per Section 4.F.(2)

Commented [EM2]: Criteria 21 and 22: Importantly, due to a risk-focused approach, the Model does not require the Licensee to include information security standards as part of its contracts with third-party services providers. It also does not require inspections or reviews of the Third Party's Information Security Practices. Instead the Model Law requires the Licensee to exercise due diligence and, under the overarching umbrella of risk analysis, as applicable, require the Third Party to implement appropriate administrative, technical, and physical measures. A more consistent criterion would be to ask if the Licensee has a process to conduct due diligence according to the risk of the third party

INCIDENT RESPONSE PLAN (Section 4H)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
23. Does the ISP contain a written incident response plan and/or ~~detailed~~ process for responding to a Cybersecurity Event?	Section 4.H.(1)
24. Is the Licensee's written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession? ~~Does the incident response plan provide clear guidance on when to initiate a Cybersecurity Event investigation?~~	Section 4.H.(1)
25. Does the incident response plan contain a list of clear and well-defined objectives?	
26. Does the incident response plan provide clear roles, responsibilities and levels of decision-making authority?	
27. Does the incident response plan address documentation and reporting regarding Cybersecurity Events and related incident response activities?~~Does the incident response plan require written assessment of the nature and scope of a Cybersecurity Event?~~	Section 4.H.(2)(f)
28. Does the incident response plan require determination of whether any Nonpublic Information was exposed during a Cybersecurity Event and to what extent?	
29. ~~Does~~ Is the incident response plan ~~provide clear steps to be taken to restore the security of any information systems compromised in a~~designed for the Licensee to promptly recover from any Cybersecurity Event? Does the incident response plan address identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls?	Section 4.H.(1) Section 4.H.(2)(e)
30. ~~Does the incident response plan sufficiently address steps to take when a Cybersecurity Event occurs at a Third-Party Service Provider where data provided by the Licensee is potentially at risk?~~	No Requirement in Model.
31. Does the incident response plan address external & internal communications & information sharing? ~~Does the incident response plan provide detailed instructions for external and internal~~	Section 4.H.(2)(d)
32. Does the incident response plan identify requirements for ~~define various levels of~~ remediation of any identified weaknesses in Information Systems and associated controls? ~~based on the severity of identified weaknesses?~~	Section 4.H.(2)(e)

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

DOCUMENTATION AND REPORTING

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
33. Does the ISP describe documentation and reporting ~~procedures for~~regarding Cybersecurity Events and related incident response activities? (Section 4.H.(f))	Section 4.H.(2)(f)
34. Does the ISP require ~~a post-event evaluation following a Cybersecurity Event?~~the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.	Section 4.H.(2)(g)
35. Does the ISP require retention of all records related to Cybersecurity Events for a minimum of five years from the date of the Cybersecurity Event?	Section 5.D.
36. Has the Licensee prepared and submitted annual certifications to its domiciliary state Commissioner/Director of Insurance? (Section 4I)	

PRIOR EXAMINATION FINDINGS

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
37. ~~Has the Licensee addressed and implemented corrective actions to any material findings from any prior examinations?~~To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, has the insurer documented the identification and the remedial efforts planned and underway to address such areas, systems or processes?	There is no reference in the Model to "corrective actions to any material findings from any prior examinations". Replaced with language from Section 4.I.

Exhibit B: Supplemental Incident Response Plan Investigation (Post-Breach) and Notification Cybersecurity Event Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 5 and 6

POST-EVENT INVESTIGATION BY LICENSEE (Section 5)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
1. Did the Licensee conduct a prompt investigation of the Cybersecurity Event?	Section 5.A.
2. Did the Licensee assess ~~appropriately determine~~ the nature and scope of the Cybersecurity Event?	Section 5.B.(2)

NOTICE TO COMMISSIONER/DIRECTOR OF INSURANCE (Section 6)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
3. Each Licensee shall notify the Commissioner as promptly as required under applicable state law, but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met: ~~Did the Licensee provide timely notice (no later than 72 hours) to the Commissioner or Director of Insurance following the Cybersecurity Event?~~	Per Section 6.A. (1) & (2), at least one of two criteria must be met for the threshold for notice to the Commissioner to be triggered.
4. Did the Notification to the Commissioner or Director of Insurance include the following information, to the extent reasonably available? (Section 6B)	
4a. The date of the Cybersecurity Event, or the date upon which it was discovered, or the Licensee became aware of the Cybersecurity Event?	
4b. A description of how the Nonpublic Information was exposed, lost, stolen or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any?	
4c. How the Cybersecurity Event was discovered?	
4d. Whether any lost, stolen or breached Nonpublic Information has been recovered, and if so, how this was done?	
4e. The identity of the source of the Cybersecurity Event?	
4f. Whether the Licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies? ~~*(If YES, did the Licensee provide the date(s) of such notification(s)?)*~~And, if so, when such notification was provided.	Section 6.B.(6).
4g. A description of the specific types of information ~~Nonpublic Information~~ acquired without authorization?	The defined term “Nonpublic Information” was not used in Section 6.B.(7)
4h. The period during which the Information System was compromised by the Cybersecurity Event?	
4i. ~~A best estimate of the number of total Consumers in this state and globally affected by the Cybersecurity Event~~? The number or best estimate of total Consumers in this State affected by the Cybersecurity Event.	The notification is not required to include an estimate of the number of customers globally affected. Replaced with language from Section 6.B.(9).
4j. ~~The results of any internal review of automated controls and internal procedures and whether or not such controls and procedures were followed~~? The results of any internal review identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed.	Not All internal reviews of automated controls are required to be included, but rather those identifying a lapse in either automated controls or internal procedures. Per Section 6.B.(10).
4k. A description of efforts being undertaken to remediate the circumstances which permitted the Cybersecurity Event to occur?	
4l. A copy of the Licensee’s privacy policy and a statement outlining the steps the Licensee will take to investigate the Cybersecurity Event and to notify affected Consumers?	
4m. The name of a contact person familiar with the Cybersecurity Event and authorized to act for the Licensee?	
5. Did the Licensee provide timely updates to the initial notification and Questions 4a-4m above? (Section 6B)	

OTHER NOTIFICATIONS (Section 6)

REVIEW CRITERIA	**NOTES (*YES, NO, NOT APPLICABLE, OTHER)***
6. ~~Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to Consumers? *(If YES, did the Licensee provide a copy of the notification to the Commissioner(s)/Directors of all affected states?)*~~ Did the Licensee comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when the Licensee is required to notify the Commissioner under Section 6A?	Section 6.C.
7. ~~Did the reinsurer Licensee provide timely and sufficient notice of the Cybersecurity Event to ceding insurers~~? If applicable, did the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred as required under applicable state law?	Section 6.E.(1)(a)
8. ~~Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to independent insurance producers and/or producers of record of affected Consumers~~? In the case of a Cybersecurity Event that involved Nonpublic Information in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, did the insurer notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner. (Unless the insurer is excused from this obligation because it did not have the current producer of record information for any individual Consumer).	Section 6.F.

THIRD PARTY SERVICE PROVIDERS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
9. Did the Cybersecurity Event occur at a Third-Party Service Provider? If yes, did the Licensee fulfill its obligations under this law? ~~*(If YES, did the Licensee fulfill its obligations to ensure compliance with this law, either directly or by the Third-Party Service Provider?)*~~	

POST-EVENT ANALYSIS

REVIEW CRITERIA	***NOTES (YES, NO, NOT APPLICABLE, OTHER)***
10. ~~What changes if any are being considered to the Licensee's ISP as a result of the Cybersecurity Event and the Licensee's response~~? Did the Licensee adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.	Section 4.I.

POLICY IN FORCE STANDARDIZED DATA REQUEST
Property & Casualty Line of Business
Private Passenger Auto

Contents: This file should be downloaded from company system(s) and contain one record for each vehicle insured under a private passenger auto policy issued in [applicable state] which was in force at any time during the examination period.

For any fields where there are multiple entries, please repeat field as necessary.

Uses: Data will be used to determine if the company follows appropriate procedures with respect to the issuance and/or termination of private passenger automobile policies in [applicable state] within the scope of the examination:

- Cross-reference with the company's MCAS data to validate MCAS reporting and review the exam data for completeness;
- Cross-reference with the claims data file to validate the completeness of the in force file; and
- Cross-reference to state(s) licensing information to ensure proper producer licensure.

Field Name	Start	Length	Type	Decimals	Description
CoCode	1	5	A		NAIC company code
PolPre	6	3	A		Policy prefix (**Blank if NONE**)
PolNo	9	20	A		Policy number
PolSuf	29	3	A		Policy suffix (**Blank if NONE**)
PolStTyp	32	3	A		Policy status type for the record (i.e., new or renewal) **Please provide a list to explain any codes used**
PolTyp	35	25	A		Type of policy, if any (i.e., standard, preferred, nonstandard) **Please provide a list to explain any codes used**
PolForm	60	10	A		Policy form number as filed with the insurance department
PrCode	70	9	A		Company internal producer, CSR, or business entity producer identification code **Please provide a list to explain any codes used**
NPN	79	6	A		National producer number
InsFirst	85	15	A		First name of the first named insured
InsMid	100	15	A		Middle name of the first named insured
InsLast	115	20	A		Last name of the first named insured
InsAddr	135	25	A		Insured street address (mailing)
InsCity	160	20	A		Insured city (mailing)
InsSt	180	2	A		Insured state (mailing)
InsZip	182	9	A		Insured ZIP code (mailing)
GarAddr	191	25	A		Vehicle garaging address
GarCity	216	20	A		Vehicle garaging city
GarSt	236	2	A		Vehicle garaging state

GarZip	238	9	A		Vehicle garaging ZIP code
PUndDrSx	247	1	A		Primary underwritten driver's sex
PUndDrMs	248	1	A		Primary underwritten driver's marital status
PUndDrEd	249	25	A		Primary underwritten driver's education level **Please provide a list to explain any codes used**
PUndDrOc	274	50	A		Primary underwritten driver's occupation **Please provide a list to explain any codes used**
VehUBI	324	1	A		Does usage based insurance apply to vehicle (Y/N)
PolPrem	325	11	N	2	Total policy premium amount (Sum of all premium for all vehicles, which includes premium, fees, etc.)
UWTier	336	25	A		Underwriting tier (policy or vehicle), if tier rating is utilized **Please provide a list to explain any codes used**
VehYr	361	4	A		Vehicle year
VehMake	365	15	A		Vehicle make **Please provide a list to explain any codes used**
VehModel	380	20	A		Vehicle model **Please provide a list to explain any codes used**
VIN	400	17	A		Vehicle identification number
VehSym	417	5	A		Vehicle symbol **Please provide a list to explain any codes used**
VehPrem	422	11	N	2	Total vehicle premium amount (Sum of all premium for the vehicle, involving all premium, fees, etc.)
BIBas	433	11	N	2	Bodily injury liability term base premium for this limit
BICls	444	6	A		Bodily injury liability driver class factor **Please provide a list to explain any codes used**
BIDev	450	6	A		Bodily injury liability deviation factors (i.e., discounts, credits, etc.) **Please provide a list to explain any codes used**
BILmtPP	456	3	N		Bodily injury limit per person (in thousands)
BILmtPA	459	3	N		Bodily injury limit per accident (in thousands)
BITrm	462	6	A		Bodily injury liability term factor
PDBas	468	11	N	2	Property damage liability term base premium
PDCls	479	6	A		Property damage liability driver class factor **Please provide a list to explain any codes used**
PDDev	485	6	A		Property damage liability deviation factors (i.e., discounts, credits, etc.) **Please provide a list to explain any codes used**
PDLmt	491	3	N		Property damage liability limit per accident (in thousands)
PDTrm	494	6	A		Property damage liability term factor
LiaCsl	500	3	N		Single liability limit (in thousands)
CLBas	503	11	N	2	Collision term base premium
CLCls	514	6	N		Collision driver class factor
CLDed	520	11	N	2	Collision deductible
CLDev	531	6	A		Collision deviation factors (i.e., discounts, credits, etc.) **Please provide a list to explain any codes used**
CLDedFct	537	6	A		Collision deductible factor
CLTrm	543	6	A		Collision term factor
CMBas	549	11	N	2	Comprehensive term base premium for this model year and symbol vehicle

CMCls	560	6	A		Comprehensive class factor
CMDed	566	11	A	2	Comprehensive deductible
CMDev	577	6	A		Comprehensive deviation factor (i.e., discounts, credits, etc.) **Please provide a list to explain any codes used**
CMFact	583	6	A		Comprehensive deductible factor
CMTrm	589	6	A		Comprehensive term factor
MPBas	595	11	N	2	Medical payments term base premium for this limit
MPCls	606	6	A		Medical payments class factor
MPDev	612	6	A		Medical payments deviation factors (i.e., discounts, credits, etc.) **Please provide a list to explain any codes used**
MPLmt	618	11	N	2	Medical payments limit
MPTrm	629	6	A		Medical payments term factor
ERSTrm	635	11	N	2	Emergency road service term base premium
ERSOpt	646	11	N	2	Emergency road service optional benefit **If codes are used, provide a list of codes along with their meanings**
RentTrm	657	11	N	2	Rental reimbursement term base premium
RentDay	668	11	N	2	Rental reimbursement daily limit
RentAgg	679	11	N	2	Rental reimbursement aggregate
UMPDBas	690	11	N	2	Uninsured motorist property damage term base premium
UMPDDev	701	6	A		Uninsured motorist property damage deviation factors **If codes are used, provide a list of codes along with their meanings**
UMPDLmt	707	3	N		Uninsured motorist property damage limit (in thousands)
UMPDDed	710	11	N	2	Uninsured motorist property damage deductible
UMPDFact	721	6	A		Uninsured motorist property damage deductible factor
UMBIBas	727	11	N	2	Uninsured motorist bodily injury term base premium
UMBIDev	738	6	A		Uninsured motorist bodily injury deviation factors **If codes are used, provide a list of codes along with their meanings**
UMBIPP	744	11	N	2	Uninsured motorist bodily injury limit per person (in thousands)
UMBIPA	755	3	N		Uninsured motorist bodily injury limit per accident (in thousands)
UMCsl	758	3	N		Uninsured motorist combined single limit (in thousands)
UIMBas	761	11	N	2	Underinsured motorist term base premium
UIMDev	772	6	A		Underinsured motorist deviation factors **If codes are used, provide a list of codes along with their meanings**
UIMPP	778	3	N		Underinsured motorist limit per person (in thousands)
UIMPA	781	3	N		Underinsured motorist limit per accident (in thousands)
UIMTrm	784	6	A		Underinsured motorist term factor
RateTerr	790	5	A		Code specifying rating territory **Provide a list of codes along with their meanings**

MVRDt	795	10	D		Date of most recent motor vehicle record (MVR) [MM/DD/YYYY]
DrDOB	805	10	D		Driver date of birth [MM/DD/YYYY]
VehSur	815	11	N	2	Vehicle surcharge amount (2 decimal places. Do not use commas or dollar signs.) **If codes are used, provide a list of codes along with their meanings**
VehDis	826	5	A		Vehicle discounts **If codes are used, provide a list of codes along with their meanings**
DrSur	831	11	N	2	Driver surcharge amount (2 decimal places. Do not use commas or dollar signs.) **If codes are used, provide a list of codes along with their meanings**
DriDis	842	5	A		Driver discounts **If codes are used, provide a list of codes along with their meanings**
AppRecDt	847	10	D		Date application received [MM/DD/YYYY]
AppProDt	857	10	D		Date application processed [MM/DD/YYYY]
InceptDt	867	10	D		Inception date of the policy [MM/DD/YYYY]
EffDt	877	10	D		Policy effective date [MM/DD/YYYY]
ExpDt	887	10	D		Policy expiration date (MM/DD/YYYY)
PdDt	897	10	D		Date policy was paid to before cancellation [MM/DD/YYYY]
CanReqDt	907	10	D		Date cancellation requested, if applicable [MM/DD/YYYY]
CanTerRs	917	64	A		Reason for cancellation/termination of coverage (i.e., lapse, insured request, company cancellation) **If codes are used, provide a list of codes along with their meanings**
CanTer	981	1	A		Who cancelled the coverage **C=Consumer and I=Insurer**
CanTerDt	982	10	D		Date policy cancelled/terminated [MM/DD/YYYY]
CanTerNt	992	10	D		Date the cancellation/termination notice was mailed [MM/DD/YYYY]
PremRef	1002	11	N	2	Amount of premium refunded to the insured
RfndDt	1013	10	D		Date premium refund mailed [MM/DD/YYYY]
RefMthd	1023	25	A		Refund method (i.e., 90%, pro rata, etc.) **If codes are used, provide a list of codes along with their meanings**
SurAmt	1048	11	N	2	Surcharge amount (2 decimal places. Do not use commas or dollar signs.)
TrafVio	1059	3	A		Number of rated traffic violations
MVAccd	1062	3	A		Number of rated vehicle accidents
EndRec	1065	1	A		End of record marker. Please place an asterisk in this field to indicate the end of the record. This must be in the same character position for every record in this table.

G:\MKTREG\DATA\D Working Groups\D WG 2019 MCES (PCW)\Docs_WG Calls 2019\SDRs\Current Drafts\PPA In Force SDR 11-27-18.docx

CLAIMS STANDARDIZED DATA REQUEST
Property & Casualty Line of Business
Private Passenger Auto

Contents: This file should be downloaded from company system(s) and contain one record for each claim transaction (i.e. paid/denied/pending/closed w/o payment) that the company processed within the scope of the examination. Include all claims open during the examination period. Do not include expense payments to vendors.

Uses: Data will be used to determine if the company follows appropriate procedures with respect to the handling of Property & Casualty claims within the scope of the examination.

- Cross-reference to annual statement claims data (amount) to ensure completeness of exam data submitted;
- Cross-reference with the company's MCAS data to validate MCAS reporting and review the exam data for completeness; and
- Cross-reference to state (s) licensing information to ensure proper adjuster licensure.

Field Name	Start	Length	Type	Decimals	Description
CoCode	1	5	A		NAIC company code
PolPre	6	3	A		Policy prefix (**Blank if NONE**)
PolNo	9	20	A		Policy number
PolSuf	29	3	A		Policy suffix (**Blank if NONE**)
ClmNo	32	15	A		Claim number
ClmPre	47	3	A		Claim number prefix (**Blank if NONE**)
ClmSuf	50	3	A		Claim number suffix (**Blank if NONE**)
Cov	53	5	A		Coverage under which claim was submitted
CovStat	58	10	A		Coverage status (e.g. paid, denied, pending, etc.) **Please provide a list to explain any codes used**
CATCode	68	6	A		Catastrophe (CAT) loss code, if applicable (**Blank if NONE**)
InsFirst	74	15	A		First name of insured
InsMid	89	15	A		Middle name of insured
InsLast	104	20	A		Last name of insured
InsAddr	124	100	A		Insured street address (mailing)
InsCity	224	20	A		Insured city (mailing)
InsSt	244	2	A		Insured resident state (mailing)
InsZip	246	5	A		Insured ZIP code (mailing)
CmtFirst	251	15	A		First name of claimant
CmtMid	266	15	A		Middle name of claimant
CmtLast	281	20	A		Last name of claimant (Entity filing proof of loss, e.g. business, etc.)

Field Name	Start	Length	Type	Decimals	Description
CmtAddr	301	100	A		Claimant street address
CmtCity	401	20	A		Claimant city
CmtSt	421	2	A		Claimant state
CmtZip	423	5	A		Claimant ZIP code
ClmStat	428	10	A		Claim status P = Paid, D = Denied, N = Pending, H = Partial Payment, C = Closed Without Payment, R = Rescinded
AdjCode	438	9	A		Internal adjuster identification code **Please provide a list to explain any codes used**
NPN	447	6	A		National (adjuster) number
LossDt	453	10	D		Date loss occurred [MM/DD/YYYY]
RcvdDt	463	10	D		First notice of loss [MM/DD/YYYY]
ClmAckDt	473	10	D		Date company or its producer acknowledged the claim [MM/DD/YYYY]
DtClmFrm	483	10	D		Date claim forms sent to claimant [MM/DD/YYYY]
NtcInvDt	493	10	D		Date of written notice to insured/claimant regarding incomplete investigation [MM/DD/YYYY]
PdClmAmt	503	11	N	2	Total amount of claim paid
ClmPay	514	50	A		Claim payee
ClmPdDt	564	10	D		Claim paid date [MM/DD/YYYY]
IntPdAmt	574	11	N	2	Amount of interest paid, if applicable
IntPdDt	585	10	D		Date interest paid [MM/DD/YYYY]
ClmDnyDt	595	10	D		Date claim was denied [MM/DD/YYYY]
ClmDenRsn	605	100	A		Reason for claim denial **Please provide a list to explain any codes used**
Subro	705	1	A		Indicate whether claim was subrogated (Y/N)
SubRecdDt	706	10	D		Date company received subrogation refund [MM/DD/YYYY]
SubAmt	716	11	N	2	Subrogation received amount
AmtSubRm	727	11	N	2	Amount of subrogation reimbursed to insured
SubRefDt	738	10	D		Date subrogation refunded to insured [MM/DD/YYYY]
TotalLoss	748	1	A		Indicate whether claim was a "Total Loss" (Y/N)
FrstLiab	749	5	N	2	Percentage of first party comparative negligence (e.g. 30%= 0.30), if applicable
ThrdLiab	754	5	N	2	Percentage of third party comparative negligence (e.g. 30%= 0.30), if applicable (repeat if necessary)
VehYr	759	4	A		Vehicle year
VehMake	763	20	A		Vehicle make **Please provide a list to explain any codes used**
VehModel	783	20	A		Vehicle model **Please provide a list to explain any codes used**
VIN	803	17	A		Vehicle identification number
NumOcc	820	2	A		Number of occupants in vehicle at time of accident

Field Name	Start	Length	Type	Decimals	Description
NetRpr	822	1	A		Repair handled through network repair shop (Y/N)
EndRec	823	1	A		End of record marker. Please place an asterisk in this field to indicate the end of the record. This must be in the same character position for every record in this table.

G:\MKTREG\DATA\D Working Groups\D WG 2019 MCES (PCW)\Docs_WG Calls 2019\SDRs\Current Drafts\PPA Claims SDR 11-27-18.docx

Attachment 4
Personal P&C Declination SDR 11-27-18

DECLINATION STANDARDIZED DATA REQUEST
Property & Casualty Personal Line of Business

Contents: This file should be downloaded from company or agency system(s) and contain one record for each policy application declined in [applicable state] at any time during the examination period.

Uses: Data will be used to determine if the company/agency follows appropriate procedures with respect to the declination of policy applications in [applicable state] at any time during the examination period:

- Cross-reference to producer data file to test for producers with declination rates that are significantly higher than or lower than the average;
- Test for unfair discrimination in declinations; and
- Test for compliance with declination notice requirements.

Field Name	Start	Length	Type	Decimals	Description
CoCode	1	5	A		NAIC company code
AppNo	6	10	A		Application number or quote number
PRCode	16	9	A		Company internal producer, CSR, or business entity producer identification code **Please provide a list to explain any codes used**
NPN	25	6	A		National producer number
LOB	31	3	A		Line of business according to annual financial statement **Please provide a list to explain LOB codes**
AppFirst	34	15	A		First name of applicant
AppMid	49	15	A		Middle name of applicant
AppLast	64	20	A		Last name of applicant
AppAddr	84	25	A		Applicant address
AppCity	109	20	A		Applicant city
AppState	129	2	A		Applicant state
AppZip	131	9	A		Applicant ZIP code
AppRecDt	140	10	D		Date application received [MM/DD/YYYY]
DeclDt	150	10	D		Date of declination [MM/DD/YYYY]
DeclRsn	160	20	A		Reason for declining application **If codes are used, provide a list of codes along with their meanings**
EndRec	180	1	A		End of record marker. Please place an asterisk in this field to indicate the end of the record. This must be in the same character position for every record in this table.

G:\MKTREG\DATA\D Working Groups\D WG 2019 MCES (PCW)\Docs_WG Calls 2019\SDRs\Current Drafts\Personal P&C Declination SDR 11-27-18.docx