CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support ~~Departments~~a Department of Insurance (~~DOIs~~DOI) in ~~their~~its response following notification or otherwise becoming aware of a cybersecurity event at a regulated insurance entity (licensee).

This guidance follows the definitions and ~~sections~~provisions of the NAIC Insurance Data Security Model Law (#668), specifically the process detailed in Section 6, "Notification of a Cybersecurity Event~~."~~," and related sections. If a state has made any changes in passing its version of Model #-668 or passed other regulations or legislation, it ~~may~~will need to adjust the guidance herein accordingly. Confidentiality parameters for reported cybersecurity event information vary depending on whether a state has adopted MDL-668, passed its own version of MDL-668, or passed its own legislation. Every state must defer to its specific confidentiality requirements.

~~Furthermore, the CERP is focused on primary actions and considerations, and it may need tailoring to suit a DOI's needs. Additionally, DOIs that implement a CERP, whether leveraging the guidance of the NAIC or not, are encouraged to ensure that CERP roles and expectations are widely understood throughout the DOI. The effectiveness of a DOI's response to a cybersecurity event may be improved if roles are clearly defined and understood. An effective CERP may assist DOIs in facilitating communication between stakeholders. In the wake of a cybersecurity event, licensees may need to address many reporting requirements either related to state or federal laws. Therefore, the CERP is written to assist a DOI's process to respond to a licensee's cybersecurity event in a way that allows it to consistently gather as much required information as possible without unduly burdening the licensee. Therefore, the CERP is also written to support and encourage the use of the Lead State concept, where possible and appropriate.~~

Scope

~~This response plan~~The CERP does not specifically address which events must be reported, as ~~cybersecurity~~ laws and regulations vary from state to state. DOIs should defer to the reporting requirements specific to their state, regardless of whether the state has adopted MDL-668, a revised version, or its own legislation.

Forming a Team and Communicating with Consumers

~~Many~~DOIs must establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive team response to cybersecurity events at regulated entities. Furthermore, many DOIs have divisions, such as consumer services sections, ~~that work together~~ to inform and protect insurance consumers. In the case of a disruptive cybersecurity event, providing the consumer services section with accurate, up-to-date information and scripts will enable better consumer assistance. ~~Such communication should be coordinated with and consistent with the messaging provided by the affected licensee prior to any consumer communication.~~

~~Therefore, DOIs may wish to have clear and defined protocols guiding external and internal communications and to establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive response to cybersecurity events at regulated entities.~~

Communication with Law Enforcement and Other Regulators

During a cybersecurity event, law enforcement agencies and other regulators may request information from the responding DOI. Engaging with law enforcement officials and regulators can benefit overall cybersecurity and inform the DOI's response, provided such communication is permitted under the relevant state regulation ~~and necessary to prevent the spread of a cybersecurity event~~.

~~Overview of Lead State ConceptLead State concept has long been in use as part of financial surveillance and in market regulation. The following text from Section 1: Examination Overview – Determining the Lead State and Subgroups of Companies, of the *Financial Condition Examiners Handbook* explains the concept:~~

> ~~Every insurance holding company system has individual characteristics that make it unique. Therefore, an evaluation of traits is required to determine how examinations for the group should be coordinated and which individual state, known as the Lead State, should assume the leadership role in coordinating group examinations. The Lead State is charged with the coordination of all financial exams for the holding company group, as well as other regulatory solvency monitoring activities (e.g., group supervision, including holding company analysis; group profile summary (GPS); assessments of the group's corporate governance and enterprise risk management (ERM) functions, etc.) as defined within the Financial Analysis Handbook.~~
>
> ~~In most situations to date, the Lead State has emerged by mutual agreement (i.e., self-initiative on its part and recognition by other states), generally as a result of the organizational structure of the group or as a result of the domicile of primary corporate and operational offices.~~

~~Additionally, the concept is also leveraged within *Market Regulation Handbook* within Chapter 4—Collaborative Actions – A Collaborative Action Guidelines says that:~~

> ~~In the case of Market Actions (D) Working Group actions, when selecting Lead States and Managing Lead States, the Market Actions (D) Working Group chair will consider at least the following criteria:~~
>
> - ~~The domestic regulator of the regulated entity;~~
> - ~~The top five premium volume and/or market share states;~~
> - ~~The referring states requested participation level;~~
> - ~~A state in which the identified issue appears to be more problematic;~~
> - ~~Geographic balance between zones;~~
> - ~~Specialized experience of a state's staff members;~~
> - ~~A state's experience in managing complex investigations or collaborative actions; and~~
> - ~~The ability to perform the duties and responsibilities of a Lead State and/or Managing Lead State.~~

~~While the Lead State concept varies in use related to cybersecurity events, it may be an appropriate means of creating efficiency while still allowing states to gather the information needed to support regulatory responses to cybersecurity events. As noted in the introduction, DOIs are encouraged to use of the Lead State concept, where possible and appropriate.~~

Understanding and Receiving Notifications and Required Information

~~As part of the information gathering process, states~~ States should be mindful that only partial information may be available~~, and~~ in the early stages of the information ~~provided may change as the~~ gathering process. As a licensee's investigation into ~~the~~ a cybersecurity event proceeds, new information may become available, and information previously provided may change.

Section 6 of ~~Model #~~MDL-668 requires licensees to notify the state insurance commissioner about reportable cybersecurity events and to provide the DOI with as many of the following 13 pieces of information ~~(from~~, set out in Section 6(B~~)~~), as possible, given the relevant state-specific required reporting timeframe:

1) The date of the cybersecurity event.
2) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.
3) How the cybersecurity event was discovered.
4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done.
5) The identity of the source of the cybersecurity event.
6) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.
7) A description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.
8) The period during which the information system was compromised by the cybersecurity event.
9) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.
10) 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.
11) A description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

12) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.
13) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

~~The items~~

A state may make changes when passing its version of MDL-668 or other legislation that varies from the requirements set out in Section 6(B) of MDL-668. In this case, the state must adjust this guidance to comply with the information it requires a licensee to report under its legislation.

Receiving the information listed above may ~~require modifications for states adopting their version of Model #668, or that have their own regulation. States may also wish to consider gathering information to help the state understand the total exposure of the incident (e.g. total individuals/policyholders, total anticipated cost (if known), and information on cybersecurity coverage in place, etc.). Such information may allow the inquiring DOI to function as a lead state regulator to respond to the cybersecurity event, which may help minimize the total number of requests to licensees.~~

~~Receiving the above information will~~ take some time, and some ~~types of~~ information may be available earlier than others. ~~Notifications can be updated after a company reports~~Event notifications should be sent out promptly without waiting for all relevant information to be gathered. After a licensee notifies the DOI of the initial cybersecurity event~~; therefore,~~, the licensee can update its notification~~ of an event should not be held up while all pertinent information is being compiled. The licensee who notified the DOI of a breach has a responsibility to update and supplement previous notifications to the Commissioner regarding material changes to previously provided information relating to the cybersecurity event as it relates to pieces of information from Section 6(B) of Model #668, to the extent possible. Where possible, DOIs should establish clear and reasonable communication expectations with the licensee to ensure material updates provided are timely. If a cybersecurity event originated at a vendor, the DOI may wish to engage with the insurer to understand the impact the origin of the event will have on the notification and event response processes.~~.

Appendix A of this document, *Cybersecurity Event Notification Form,* provides an optional form that can be used to help states collect information.

The licensee notifying the DOI of a breach is responsible for reporting updated data, as required, in accordance with relevant state law. If the licensee in question is the DOI's domestic licensee, it is the DOI's responsibility to ensure the ~~company~~licensee provides as much of this information as possible. ~~It may also be appropriate to request information in addition to the examples listed above, including a corrective action plan and status of consumer notifications, which can benefit the DOI's ongoing supervisory work.~~

~~Appendix A—Cybersecurity Event Notification Form provides an optional form that can be used to help states collect information.~~

The license is not required to provide specific documents, such as an investigatory report or other documentation, to comply with the information reporting requirements of Section 6(B). While an investigatory or other document may contain the information required by Section 6(B), Section 6(B) does not require that the documentation itself be provided to the DOI. MDL-668 requires that the licensee need only send a description of the required information.

If a DOI determines that it needs to review the underlying documentation, the DOI may want to consider bringing an investigation pursuant to MDL-668 Section 7(A) in the event this section is applicable. Information received pursuant to an investigation brought under Section 7(A) is subject to greater confidentiality protection. If Section 7(A) or a similar section is not applicable, the DOI may consider opening a limited-scope investigation or another similar style of examination that provides explicit confidentiality protection to a licensee.

Notwithstanding anything provided in this CERP, a DOI must comply with its responsibilities under MDL-668 Section 8, "Confidentiality," or with the confidentiality requirements in its own legislation, and ensure that all reported cybersecurity event data is properly secured.

Process for Responding to Cybersecurity Events

~~There may be at least~~ A DOI's process of responding to a licensee's cybersecurity event should allow it to consistently gather as much required information as possible without unduly burdening the licensee, and a DOI's engagement with a licensee may vary depending on the facts and circumstances of each cybersecurity event. To illustrate, consider three general points where a DOI can engage with a licensee after a cybersecurity event: 1) upon receiving notification or becoming aware of the event; 2) after the DOI's initial investigation; or 3) ~~or~~ upon the DOI's completion~~. A DOI's engagement with a licensee may vary based on the facts and circumstances of each cybersecurity event.~~ of the investigation. Some questions ~~to~~a DOI should consider when making ~~such a~~the determination ~~as to the appropriate scope of the DOI's engagement are as follows~~of when to engage with the licensee include:

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry (e.g. through the involvement of third-party software many insurers use)?
- Has the licensee lost the ability to process transactions? Can they process claims? Premiums?
- Can the licensee communicate with policyholders? Are their telephones, email, and website working?
- Has the licensee engaged in any general communication with policyholders? Is the licensee able to post a notice on its website? If so, when was the notice posted?
- Has law enforcement responded to the licensee's situation? Are they on-site?
- Are there other professionals on-site assisting with the recovery? What are their roles?

For a cybersecurity event that has been remediated and ~~has~~had a limited impact on daily operations and information technology (IT) operations, the DOI may ~~let~~consider allowing the licensee's investigation to run its course before stepping in to obtain ~~the~~any necessary information.

Cybersecurity events that have occurred at a third-party service provider require a different approach by the DOI. Often, a licensee will avail itself of MDL Section 6(D)(3), which allows a third-party service provider to fulfill its notification or investigative requirements pursuant to the terms of an agreement with a licensee. In any event, the licensee must acquire the information required to be reported from the third-party service provider.

If a DOI determines that further investigation is appropriate~~, then examining~~ to ensure policyholder data is secured, an examination by the DOI of the licensee's response and remediation of the cybersecurity event ~~to ensure policyholder data is secured~~ may be warranted. There are several investigative options available to ~~state insurance regulators, which are~~a DOI, summarized in a document titled "*Summary of Cybersecurity Tools,*" which is maintained by the NAIC's Cybersecurity (H) Working Group under the "Documents" tab on the Working Group's page~~—"*Summary of Cybersecurity Tools*." At a summary level, those~~. These tools include:

- Using the Powers of the Commissioner to examine and investigate and take appropriate enforcement action Under Section 7(A) and (B) described in ~~Model #~~MDL-668, if adopted and in effect;
- ~~Investigating~~ Bringing an investigation via the exam process described in the *NAIC's Financial Condition Examiners Handbook*; and
- ~~Investigating via~~Using the following checklists included in the NAIC's *Market Regulation Handbook*~~:~~ *to assist the DOI's inquiry:*
  - "Insurance Data Security Pre-Breach Checklist~~",~~," and
  - "Insurance Data Security Post-Breach Checklist"."

~~Ad-hoc inquiry, which may leverage the insights in~~

- ~~—~~A DOI must be prepared to address concerns about the ~~NAIC's *Cybersecurity Vulnerability Response Plan*~~.

confidentiality and protection of cybersecurity event information that has been reported to it, either under MDL-668 Section 8 or under state confidentiality and information privacy legislation. When a licensee asserts that information required ~~in~~by MDL-668 is exempt ~~due to~~ from reporting because it falls under the attorney-client privilege, or ~~asserts~~that information ~~requested is~~required by MDL-668 constitutes a trade secret~~ or is otherwise confidential~~, a DOI ~~should~~must consult its legal counsel as to how to proceed.~~ A DOI may need to be prepared to address concerns about confidentiality and the protection of their cybersecurity event information noting that Section 8(A) of MDL-668 provides confidentiality protections to the information submitted under Section 6(B). While every state has their own confidentiality and privacy regimes relating to cybersecurity event information, MDL-668 provides explicit confidentiality protection for most event information provided, as found in Section 8(A).~~

If a licensee ~~is concerned~~expresses concern about the sensitive nature of a ~~specific~~particular document (~~e.g. their~~ for example, a forensics ~~reports or other sensitive information)~~report), a DOI ~~may need to~~should consider performing a formal investigation ~~described under~~ pursuant to Section 7(A) of MDL-668. As discussed above, documents received pursuant to Section 7(A) of MDL-668~~, which provides licensees with~~ are subject to greater confidentiality~~.~~ protection than is provided by Section 6(B) of MDL-668. If a state's version of MDL-668 does not ~~have a~~ provide confidentiality protections comparable ~~confidentiality protection~~to those provided by Section 7(A) of the MDL-668, a limited-scope examination may offer a licensee similar confidentiality protection ~~to the licensee. To the extent a DOI relies on third-party consultants for such investigations or examinations, DOIs may need to take steps to ensure that information viewed by the third-party consultants remains subject to the confidentiality provisions afforded under MDL-668.~~.

How to Receive Notifications and Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. ~~Options include a secured email inbox, an online form such as a PDF, or using a dedicated secure portal to complete an online form that stores the information in a database. Before a cybersecurity event,~~ DOIs should take reasonable steps to ensure they have proper communication ~~and security~~ protocols and tools in place ~~if the transmission~~in advance of ~~information is necessary.~~becoming notified or aware of a cybersecurity event. Communication channels ~~and storage options~~ established for event notification should provide ~~reasonable~~ security ~~of the~~for cybersecurity event data ~~–~~in ~~–~~transit and data ~~-~~at ~~–~~rest, commensurate with the sensitivity of the reported information. ~~The security of communication protocols and channels should be reassessed periodically.~~

~~Communication preferences within each DOI should generally be proactively communicated by DOIs with instructions on state webpages accessible to licensees for how and where notifications should be submitted.~~

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if any, with a form requesting information. As noted above, information may be available at different times throughout the ~~cybersecurity~~cyber event lifecycle, and notifications can be updated after a licensee makes the initial report.

Appendix A: Sample Template (This is available in Excel~~).~~):

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Information Provided		Company Response
Company Name		
1	Date of the cybersecurity event.	
2	Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.	
3	How the cybersecurity event was discovered.	
4	Whether any lost, stolen, or breached information has been recovered and if so, how this was done.	
5	The identity of the source of the cybersecurity event.	
6	Whether licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.	
7	Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.	
8	The period during which the information system was compromised by the cybersecurity event.	
9	The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.	
10	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.	
11	Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.	
12	A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.	
13	Name of a contact pers and authorized to act fo	