CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support a Department of Insurance (DOI) in its response following notification or otherwise becoming aware of a cybersecurity event at a reguciatiE(n.1(te)6(d iciation)s,(twill 8e5.7(Tw[(is))-.6(t1-.1(s58e5c))6(e e8 Tm-e))-.67()1(te3.7((D)-.0(As.7(fi(te1)6(e e58e5.7(Tw[cia6e)i)-54(.582 t-1711.2031.2

---

with compliance.

This guidance follows the definitions and provisions

Appendix A of this document, *Cybersecurity Event Notification Form,* provides an optional form that can

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 had a limited impact on daily operations and information technology (IT) operations, the DOI may consider allowing the licensee's investigation to run its course before ~~stepping in~~engaging to obtain any necessary information.

similar confidentiality protection.

How to Receive Notifications and Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. DOIs should take reasonable steps to ensure they have proper communication protocols and tools in place in advance of becoming notified or aware of a cybersecurity event. Communication channels established for event notification should provide security for cybersecurity event data-in-transit and data-at-rest, commensurate with the sensitivity of the reported information.

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if any

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

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

	Information Requested	**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	
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 **of MDL-668]**.	
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