OUTLINE FOR INCIDENT RESPONSE FOLLOWING A CYBERSECURITY EVENT
CYBERSECURITY (H) WORKING GROUP

I. Introduction

Paragraph defining the purpose of the response plan, considerations when choosing a response team, sections the plan will cover.

II. Communication with other States/Federal Regulators

This section should include examples of when a state needs to reach out to other states or to federal regulators.

III. Initial Notification by Domestic

This section should discuss a means for the licensee to report an incident. This section could suggest the various methods of reporting.

IV. Meetings

The number of meetings will be determined once the depth of the cybersecurity incident is determined; however, an initial meeting should be set up so the response team at the DOI to learn about the event, reports regarding contacting law enforcement, and to determine if follow-up meetings are needed.

V. Communication with the Firm Handling the Incident

This section should include details received from the firm handling the incident regarding the details of the incident, as well as the steps taken to remediate the incident and notify affected consumers.

VI. Organizational Security

This section should contain details of Organizational security, including, but not limited to: Training, logical security, operational security, physical security, network security, application security, and vulnerability assessment.

VII. Risk Assessment

This section should provide a description of how the licensee assesses risk. Example could be how a company assesses risk of third-party vendors and software, use of a third-party to assess cyber resilience, including but not limited to table-top exercises.

VIII. Audits

This section should include any policy or program audits.

IX. Communication with Consumer

This section should include information that should be communicated to a consumer following a breach.

X. Summary of Regulator Tools

XI. Coordination of Communication

XII. Information Gathering Template

This section should include the types of information that are important to gather following a cybersecurity incident.