Cl Survey Response Summary

Richard Mroz
Chair
Critical Infrastructure Committee
February 12, 2017
Emergency Management Frameworks

<table>
<thead>
<tr>
<th>Framework</th>
<th>Commissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Hazard Planning and Response</td>
<td>21</td>
</tr>
<tr>
<td>Regional All Hazard Planning and Response</td>
<td>17</td>
</tr>
<tr>
<td>State Fusion Centers</td>
<td>22</td>
</tr>
</tbody>
</table>

- **NA**: No data available
- **Yes**: Indicates the presence of the framework
- **No**: Indicates the absence of the framework
Cyber Security

Engage Utilities?

- Yes: 86%
- No: 5%
- Not Engaged: 9%

Issued Orders?

- Yes: 55%
- No: 45%
Exercises

Has your state performed a table top or other form of exercise that involves public utilities?

- Yes: 11
- No: 5

Has your state conducted an exercise based on a cyber security scenario?

- Yes: 11
- No: 8
Is cyber threat information voluntarily shared with your commission by regulated utilities?

- Yes: 12
- No: 8
- NA: 2

Between state agencies?

- Yes: 12
- No: 8
- NA: 2

Between the commission and federal partners?

- Yes: 12
- No: 8
- NA: 2
Does anyone on your commission have a security clearance?

- Yes: 12
- No: 9

If not, is the commission in the process of obtaining a security clearance for one or more commissioners?

- Yes: 8
- No: 4

For commission staff?

- Yes: 8
- No: 4
Ground rules established regarding which state officials should receive confidential or sensitive cyber information, and what steps should be taken to protect it.

Authorities exist that allow the commission to deem certain sensitive data as confidential, i.e., “not a public record,” and, thereby, protect it from public disclosure.