



## WS 101: Creating Cybersecurity and Incident Response Plans

### AGENDA

September 29, 30, and October 1, 2020

10:00am - 12:30pm ET (*each day*)

<p><b>Session 1</b> <b>Cybersecurity</b> <b>Planning - Part 1</b></p> <p><b>September 29</b></p>	<p>Introductions &amp; orientation to the series (10 minutes)</p>	<p>→ Cybersecurity planning: How developing a solid cybersecurity plan gives your district the big picture of how you should keep the district's data and systems secure.</p>
	<p>Laying The Foundation (75 minutes)</p>	<p>→ Why plan? The reasons for and benefits of cybersecurity planning (20 mins)</p> <p>→ Preparing to plan: Conducting a Risk Assessment, leveraging the CoSN S2 assessment as a resource (20 mins) Amy</p> <p>→ Start with a framework: Security standards, regulations, and templates (20 mins)</p> <p>→ Breakout Session: You have artifacts - let's discuss what you've already got (15 mins)</p>
	<p>Building the Plan (60 minutes)</p>	<p>→ What is working now? Plan for maintenance and replacement (20 mins)</p> <p>→ Critical risk &amp; gap analysis: What needs to be fixed right now? (20 mins)</p> <p>→ Long term improvements: Roadmap to future security improvements (20 mins)</p>
	<p>Homework (5 mins)</p>	<p>→ Take away assignments to collect artifacts and start using a supplied template to build a plan.</p>

**Session 2  
Cybersecurity  
Planning - Part 2  
September 30**

Welcome to Day 2 (5 minutes)	
Breakout Groups (20 mins)	→ Sharing the plans in progress
Using the Plan (40 mins)	<ul style="list-style-type: none"> <li>→ Getting support: Socializing the plan (20 mins)</li> <li>→ Implementing, maintaining and updating the plan (20 mins)</li> </ul>
Incident Response Planning (80 mins)	<ul style="list-style-type: none"> <li>→ What's an Incident? What are you preparing for? The incident response cycle. (20 mins)</li> <li>→ Planning for the unknown: The limitations of incident response planning (20 mins)</li> <li>→ Building a plan (40 mins) <ul style="list-style-type: none"> <li>◆ Response planning</li> <li>◆ Communications planning</li> <li>◆ Roles &amp; responsibilities</li> </ul> </li> </ul>
Homework (5 mins)	→ Begin building your incident response plan using the provided template.

**Session 3  
Cybersecurity  
Planning - Part 2  
October 1**

Welcome to Day 3 (5 minutes)	
Breakout Groups (20 mins)	→ Share your incident response plan in progress
Preparing to use the plan (60 minutes)	<ul style="list-style-type: none"> <li>→ Key players: Insurance, general counsel, communications director (20 mins)</li> <li>→ Set the stage: Sharing the plan (20 mins)</li> <li>→ Train &amp; practice: Rehearsing your incident response (20 mins)</li> </ul>
Implementing your plan (35 minutes)	<ul style="list-style-type: none"> <li>→ Triggering the plan: Knowing when to use it (15 mins)</li> <li>→ Recovering from an incident &amp; lessons learned (20 Mins)</li> </ul>
Breakout groups (15 mins)	→ Next steps: Identify your top 3 next steps to successfully complete and use your security and incident response plans
Group reflection & closure (10 mins)	