CYBER DISRUPTION RESPONSE PLANNING GUIDE

Recommendations	
✓	Identify all partners from across government, industry and non-profits to build a network of stakeholders related to cyber disruption planning.
✓	Establish positive collaboration among various stakeholders now - well in advance of a cyber disruption. There should be frequent non-crisis interaction in order to develop the necessary trust relationships that will be fully exercised during the stress of a real crisis.
✓	Integrate cyber disruption planning with emergency management operations.
✓	Establish the necessary governance for a regional cyber disruption plan. Governance will clearly define lines of responsibility for advisory and decision making roles based on effects and types of cyber disruption events.
✓	Establish a priority for activities based on near-term, medium term and long term time lines.
✓	Establish a means for sharing ideas across regional cyber disruption initiatives in order to leverage the best practices and innovative approaches.
✓	Identity vulnerabilities in current infrastructures including computer networks.
✓	Develop a strategy for continuity of communications within government and with its external partners specifically addressing the loss of telecommunications including internet and wireless networks.
✓	Develop communication and coordination procedures to ensure timely and effective response in the event of a cyber disruption.
✓	Develop contingency plans, alternative action plans considering secondary effects of regional emergencies and secondary effects of cyber disruptions.
✓	Identify what resources can be brought to bear from across the cohort of partners based on scenarios and effects.
✓	Carefully examine supply chains, particularly those that are relied upon by all partners. If the supply chain is broken for one partner, that is most likely the circumstance for other partners.
✓	Insure backup communications networks are ready to launch and that such networks can sustain for some period of time. Over time that sustainability should be continually improved.

✓	Develop test plans for coordinating response across several or more infrastructures.
✓	Begin to identify tactical and medium term strategies for addressing loss of power and telecommunications. Consider developing regional and local power grids that are isolated from the internet and would provide dependable power in the case of a blackout or brownout. Such a regional grid would be developed under cross-jurisdictional collaborative.
✓	Develop, maintain and test a cross functional process flow that describes how stakeholders will interact at all threat levels. A starting point for this effort could be existing cross functional process flows for cyber incident management. Such a process could be scaled up to include all necessary players to deal with a cyber disruption.
✓	Incorporate resiliency measures into the enterprise portfolio for processes, systems, data and information assets, hardware, cloud services, shared services. Attribute the level of criticality for all IT assets.
✓	Incorporate resiliency requirements into every project, program and management initiative.