**Summary of the Draft Cyber Annex to the Regional Emergency Coordination Plan**

**Introduction:**

Over the past several months, the Chief Information Security Officers (CISO) Subommittee has taken the lead in developing a draft Cyber Annex to the Regional Emergency Coordination Plan (RECP). The purpose of the draft Cyber Annex to the Regional Emergency Coordination Plan (RECP) is to build upon existing communication protocols (see flow chart below) and support the region’s public policy in preventing and protecting against, responding to, and recovering from any cyber incident of regional significance. The draft Annex is intended to augment the RECP in guiding the region’s overall preparation for and response to cyber-related emergencies and disasters. Regional stakeholders will use this annex to assist them in their planning and responding activities for all relevant cyber emergencies.

**Draft Annex Planning Assumptions:**

Cyber incidents occur every day. Preventing and protecting against, responding to, and recovering from a cyber incident is different and unique from more traditional emergency events. This is because the current environment is a steady state of malicious activity. The range of consequences involving a cyber-incident is also significant. The risk of a singular cyber-incident having a cascading effect on critical infrastructure, including the operations of those systems and the ability to deliver essential services to the region and its citizens is an ongoing concern.

Because the steady-state cyber environment experiences on-going and constant malicious activity, approaching regional cybersecurity is different than other approaches to emergency management. Unlike physical disasters, cyber events occur constantly. The key to preparedness – in alignment with PPD-8 – is protecting, preventing, containing, managing, and recovering while ensuring the resiliency of critical systems. The NIST Cybersecurity Framework describes a phased approach of identify, protect, detect, respond and recover.

Each jurisdiction has its own best practices, procedures, and utilizes Computer Emergency Response Teams/Computer Incident Response Teams (CERT/CIRT) policies appropriate to its needs. The draft Cyber Annex is intended to complement existing programs, policies and procedures, and assist key stakeholders within the region—including Chief Information Officers, Chief Information Security Officers, and Emergency Managers—in responding to an incident and mitigating its consequences and effects.

This Annex will also support the communication of information before, during, and after an incident to support local jurisdictions and organizations in determining appropriate actions based on the collective regional knowledge of the situation. The Cyber Annex will also support information sharing among jurisdictions related to the need for local, regional, state, or federal assistance.

**Key Coordination and Operations Recommendations:**

1. Establish the CISO Committee as the central resource for NCR jurisdictions for coordination of cyber activity. The CISOC will provide support to jurisdictions as they implement the NIST Cybersecurity Framework and develop their cyber risk management current profile. The CISOC will coordinate COG efforts to normalize cyber preparedness and response plans with existing emergency management procedures and systems (i.e., NIMS).
2. Designate a regional cyber incident coordinator to serve as a central point for coordination of NCR cyber efforts.
3. Encourage jurisdictions to create a profile of their current cyber risk management process by applying the NIST Cybersecurity Framework.
4. Work with DHS to explore the possibility of embedding a local jurisdictional representative in the National Cybersecurity and Communications Integration Center (NCCIC).

