BACKGROUND

In July 2017, the Mid-America Regional Council (MARC) hosted a series of facilitated planning meetings to discuss the potential development of a regional cybersecurity strategic framework.

This framework would outline actions that MARC and the region could take to strengthen the capacity of local governments to address cybersecurity threats in a coordinated effort.

Steve Arbo, Lee’s Summit, Missouri city manager and co-chair of the Regional Homeland Security Coordinating Committee (RHSCC) led the initiative, and the planning team members represented a blend of city and county managers, information technology security specialists, a risk/liability executive, cybersecurity technicians, first responders, emergency managers, and post-graduate level cybersecurity program administrators.

The scope of work/purpose for the planning meetings included:

1. Create a leadership group that can build capacity and provide sustainable commitment.
2. Create a regional strategic framework (vision, values and guiding principles).
3. Build the key components of a first-year cybersecurity work plan.
4. Discuss a short-term funding strategy, identifying resources necessary to accomplish the first-year work plan.

This summary describes the results of these facilitated discussions.

VISION STATEMENT

Local governments can successfully operate under constant technological change and cybersecurity threats, allowing citizens to fully access government services. The Kansas City region, in a collaborative effort, will create a secure environment where local governments can maintain resilient infrastructure, public trust and support that benefits from organizational interconnectivity and innovation.

VALUES & PRINCIPLES

To be successful in this endeavor, the leadership work group participants understand the importance of ensuring the integrity of technology connections that transcend current local government and agency barriers and that build on strong working relationships, while maintaining technological standards.

Our relationships must be based upon:

- Trust and the ability to share resources to achieve a mutually positive outcome.
- Recognition of the benefit of working in a collegial manner.
- Developing a culture of proactive thinking in order to minimize costly reactive efforts.
- Remembering that local government services openness and accountability must be balanced with the need to create a secure environment.
- The ability to sustain public trust and confidence.
- Addressing cybersecurity challenges without interfering in the provision of dependable and reliable local government services.
- The ability to pursue innovative technology opportunities within a secure environment.
ACTION STEPS  Our vision can be achieved by implementing six targeted actions:

**1 IDENTIFY AND ESTABLISH BEST PRACTICES FOR CYBERSECURITY PLANNING.**
- Form a regional work group to provide leadership, guidance and commitment.
- Determine an ongoing system to identify and share information on a regional basis.
- Conduct individual local government threat assessments to determine individual community and regional levels of risks.
- Establish minimum operational standards as a baseline for the regional initiative.
- Gather data on current practices.
- Design a proof-of-concept document that examines the feasibility of best practices prior to regional adoption.
- Promote and encourage region-wide adoption of best practices.

**2 DESIGN AND IMPLEMENT REGIONAL COMMUNICATIONS STRATEGIES**
- Create a common regional cybersecurity identity to ensure strong communications.
- Develop a set of communication processes that allow known and perceived cyber threats to be shared on a “real time” basis.
- Use communications channels currently offered by the federal government through DHS.
- Create public response information (message maps) that public information officers can use to communicate with the public about cyberattacks and threats to the region and/or local community.
- Develop an ongoing communication program for both internal and public purposes to encourage safe practices and prevention.

**3 CREATE COLLABORATIVE TRAINING OPPORTUNITIES TO BUILD A HIGH QUALITY WORKFORCE**
- Gather and share information on currently available high-quality end-user security training programs for local governments.
- Deploy employee training programs that inform, educate and encourage safe technology behaviors.
- Design and deploy educational materials and presentations for elected officials and the public.
- Develop a regional strategy to produce a workforce pipeline of highly qualified candidates to support local and regional cybersecurity efforts in local government.

**4 CREATE A SHARED SERVICES MODEL TO SUPPORT LOCAL GOVERNMENTS**
- Research national and local shared services models to find successful strategies for replication.
- Explore opportunities for shared procurement of training products, consulting services, software, and third-party security services.
- Gather information to create a regional inventory of current practices in cybersecurity risks and prevention techniques.

**5 IMPROVE REDUNDANCY AND RESILIENCE THROUGH MUTUAL AID NETWORKS AND SHARED SERVICES**
- Build a network of disaster recovery sites that provides cost-effective redundancy and resiliency and is especially beneficial to smaller jurisdictions.
- Establish an incident response team made up of a cadre of trained professionals who can deliver immediate response guidance.
- Combine efforts where feasible to share expertise, services and resources.

**6 ESTABLISH A SUSTAINABLE FUNDING SOURCE TO SUPPORT REGIONAL RESPONSE TO CYBER THREATS.**
- Use the regional cybersecurity leadership work group to determine the level of resources needed in the short term (first year).
- Devise a business plan that describes regional efforts, start-up and maintenance costs.
- Submit proposals to participating jurisdictions and philanthropic organizations for financial support.

**NEXT STEPS**

The Regional Cybersecurity Leadership work group will use the action steps detailed above to develop a timeline and first-year work plan. The group will meet in September to discuss priorities and potential funding strategies.