RESILIENCY FACT SHEET

Government and public safety entities rely on voice and data communications networks to fulfill their missions, yet communications continuity planning often overlooks one of the most critical and vulnerable parts of these networks: the local access network. The local access network is the "last mile" connection between an organization's on-site communications infrastructure and the service provider's network. An incident such as a cable cut, flood, or damage to the service provider's facility can completely disrupt the local access network, leaving an organization unable to perform critical functions.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD) helps organizations mitigate threats to communications continuity and supports resilient, "always available" communications. ECD latest guidance focuses primarily on local access because this area of the network typically has the least diversity, in contrast to metro and national networks, which tend to have much greater diversity. However, ECD's capabilities extend beyond local access to address risks associated with infrastructure architecture, emerging technologies, and cybersecurity.

Resiliency Resources

Recently, ECD published *Public Safety Network Communications Resiliency Self-Assessment Guidebook* and *Public Safety Communications Resiliency: Resiliency Ten Keys to Obtaining a Resilient Local Access Network*. These resources establish a process to assess threats and vulnerabilities to communications networks, enabling organizations to conduct self-assessments and identify ideal mitigation solutions.

ECD has been performing route diversity assessments since 2002. Numerous public safety answering points, emergency operations centers, and federal departments and agencies have benefited from these assessments. Figure 1 is an example of the type of information conveyed in the ECD guidance.

Example 1
Route Diversity with Cabling in Close Proximity

Example 2
Route Diversity with Physically Separate Cabling

Example 3
Route Diversity with Physically Separate Cabling and Separate Central Offices

Figure 1. Route Diversity Examples

UNDERSTANDING COMMUNICATIONS CONTINUITY

Communications continuity is a network's ability to withstand damages, thereby minimizing the likelihood of a service outage.

Three key elements ensure continuity:

- **Route Diversity**—Communications routing between two points over more than one geographic or physical path with no common points
- **Redundancy**—Additional or duplicate communications assets share the load or provide back-up to the primary asset
- **Protective/Restorative Measures**—Protective measures decrease the likelihood that a threat will affect the network, while restorative measures, such as ECD's Telecommunications Service Priority, enable rapid restoration if services are damaged or destroyed

Benefits

ECD maintains technical expertise and shared experience from previous assessments to ensure that requesting organizations benefit from the most up-to- date information and best practices.

ECD supports mission-critical services and resiliency assessments can assist an organization in:

- Ensuring continuity of service in the event of an emergency
- Justifying network operations and improvement funding requests
- Increasing organizational control
- Prioritizing areas for network improvement
- Fulfilling mandated and/or organizational diversity assessment requirements

Resource Content

ECD resiliency publications, the *Self-Assessment Guidebook* and *Ten Keys Guide*, introduce the resources and necessary steps to assess resiliency threats and vulnerabilities to communications networks, enabling organizations to identify ideal mitigation solutions, and employ resiliency best practices.

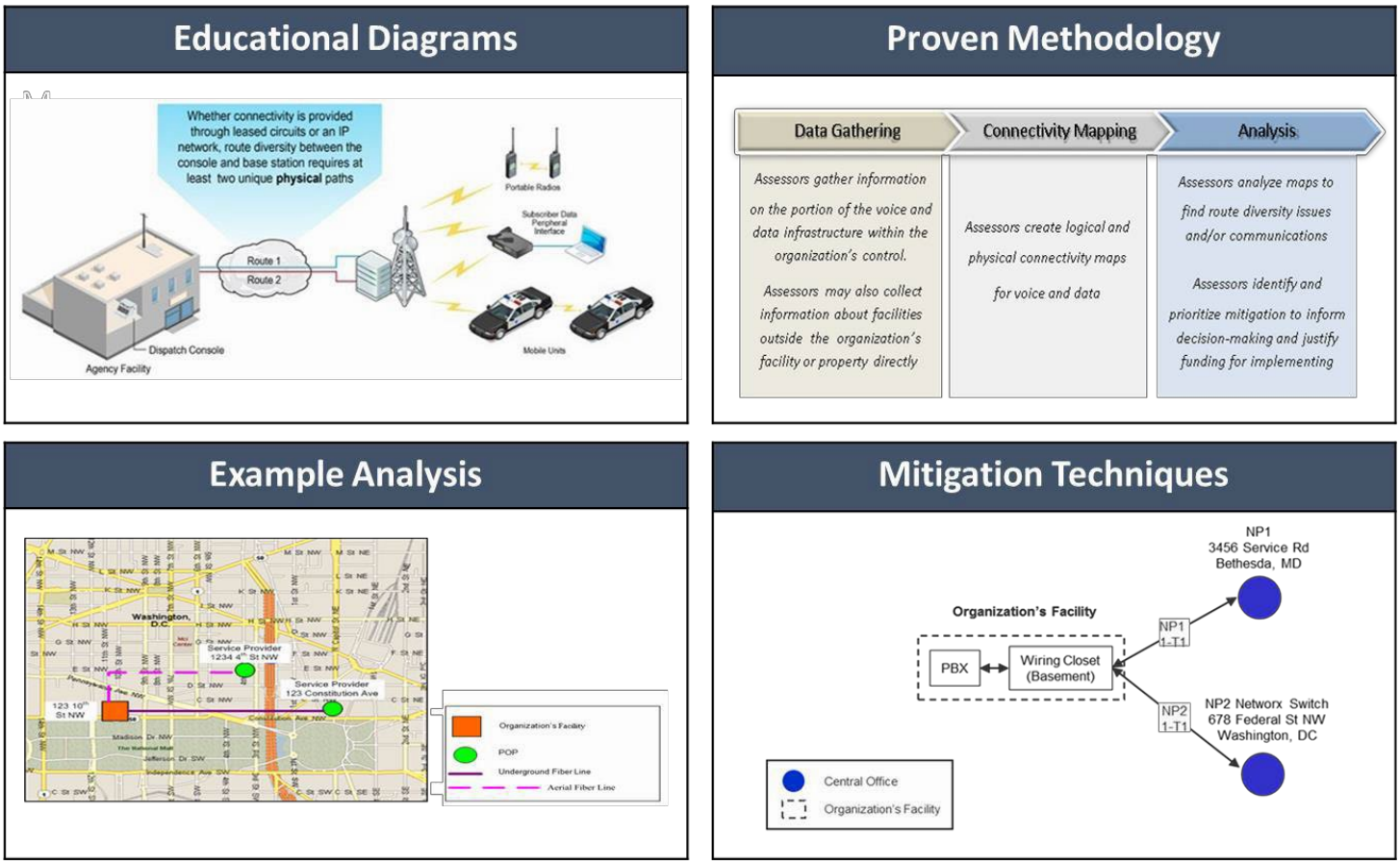

Figure 2. Examples of Content

FOR ADDITIONAL INFORMATION

Please contact **OEC@hq.dhs.gov** or visit
https://www.dhs.gov/cisa/emergency-communications-division