Public Safety Communications Network Resiliency Self-Assessment Guidebook

November 2018

SAFECOM™

NCSWIC®

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

EXECUTIVE SUMMARY

Federal, state, local, tribal, and territorial government and public safety entities rely on voice and data communications networks to achieve their missions. Yet, one of the most critical and vulnerable parts of these networks is often overlooked: 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. In the event of an emergency, such as a cable cut, flood, or damage to the service provider's facility, the local access network may be lost, leaving an organization unable to perform critical functions. This document provides guidance for public safety planners to assess and improve resiliency on voice and data networks.

Communications resiliency means a network can withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements: route diversity, redundancy, and protective/restorative measures.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Emergency Communications Division (ECD) helps organizations address issues related to communications resilience. ECD has conducted significant research and established methodologies to assist organizations in maintaining "always available" communications. This document addresses local access because this area of the network typically has the least resilience, while urban and national networks tend to have much greater resilience. ECD's focus on resilience extends beyond local access to risks associated with infrastructure architecture, telecommunications and electric power interdependencies, emerging technologies, and cybersecurity.

Conducting a resiliency assessment of public safety telecommunication resources that enable and support mission-critical services ensures:

- Continuity of service in the event of an emergency
- Increased organizational control
- Prioritization of areas for network improvement
- Justification for network improvement funding requests
- Fulfillment of organizational diversity assessment requirements

ECD has been performing resiliency assessments since 2002. These efforts are grounded in technical expertise and previous experience helping organizations with resiliency. ECD assistance improves communication continuity within and between emergency operations centers, public safety answering points, and other critical public safety entities.

Table of Contents

1.0 INTRODUCTION

Federal, state, local, tribal, and territorial government and public safety entities rely on voice and data communications networks to achieve their missions. Yet, one of the most critical and vulnerable parts of these networks is often overlooked: 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. This document provides guidance to assess and improve resilience of local access networks. Capabilities within the public safety community, such as owned or shared networks, public safety answering points (PSAP), public safety communications centers and emergency operations centers, deliver essential services to the public and other critical infrastructure sectors.

This document also provides a self-assessment methodology for public safety entities (hereafter referred to as "organizations") to identify and address potential points of failure in their communication networks by evaluating the local access networks of their primary and alternate operating facilities. The methodology describes the process of gathering data on network infrastructure, creating logical and physical network maps, and choosing resiliency solutions based on the network maps. Overall, the process helps organizations increase the continuity of communications systems by identifying new resilient solutions that ensure organizations can continue to support operations during emergencies.

2.0 COMMUNICATIONS RESILIENCY

Communications resiliency means a network is able to withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements:

- **Route Diversity**
  Route Diversity is defined as communications routing between two points over more than one physical path with no common points.
- **Redundancy**
  Redundancy means that 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 priority telecommunication services, enable rapid restoration if services are lost or congested.

While the successful implementation of these three elements combined will provide optimal communications resilience, this document focuses primarily on assessing the amount of diversity present in a network to help public safety entities identify and address potential points of failure in their communications networks. Figure 1 illustrates a route diverse communications network between an organization's facility and a telecommunications Central Office (CO) that includes physically separate points of entry or exit at the organization's facility, two physically separate cabling paths to the CO, and physically separate points of entry or exit at the CO. Although the definition of route diversity does not include a standard for route separation distance, actual implementation of route diversity suggests the

greater the distance of separation, the greater the benefit. For example, if the separate points of entry are next to each other, route diversity still exists (Example 2 in Figure 1); however, this may not be the best implementation of route diversity in practice. A better implementation of route diversity is shown in Figure 1 Example 2 where the cabling paths have significant physical separation. Figure 1 Example 3 demonstrates the best example of route diversity in Figure 1, as the routes are both physically separate and a choice can be made between two COs for routing.

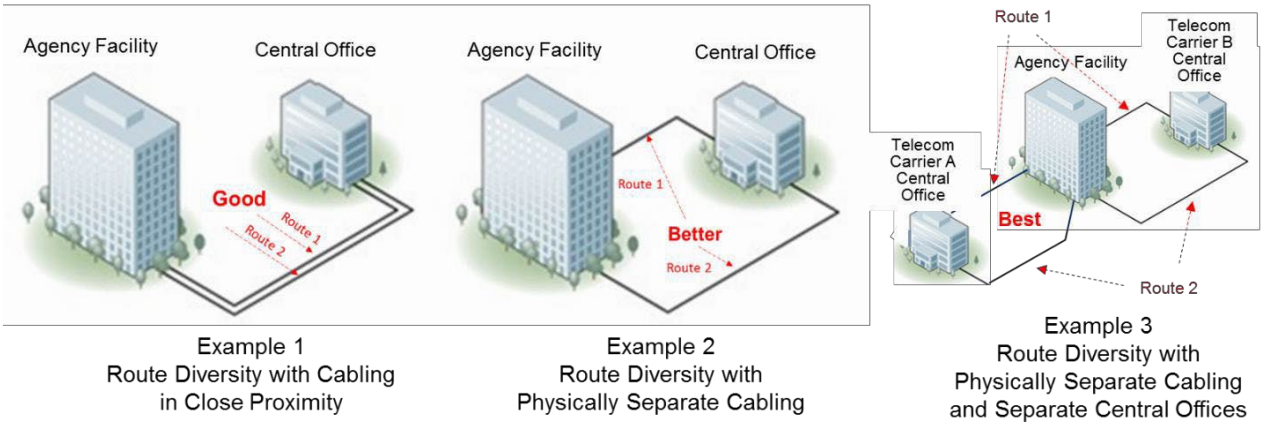

Figure 1. Route Diversity Examples

As shown in Figure 2, land mobile radio (LMR) network route diversity involves at least two unique paths between the console and the base station(s)/repeater sites, and/or the central controller and the geographically dispersed repeater/tower sites whether provided through leased circuits or an Internet protocol (IP) network. The same concepts for diversity demonstrated in the figures throughout this paper between an agency facility and CO apply also to the communications paths of LMR networks.

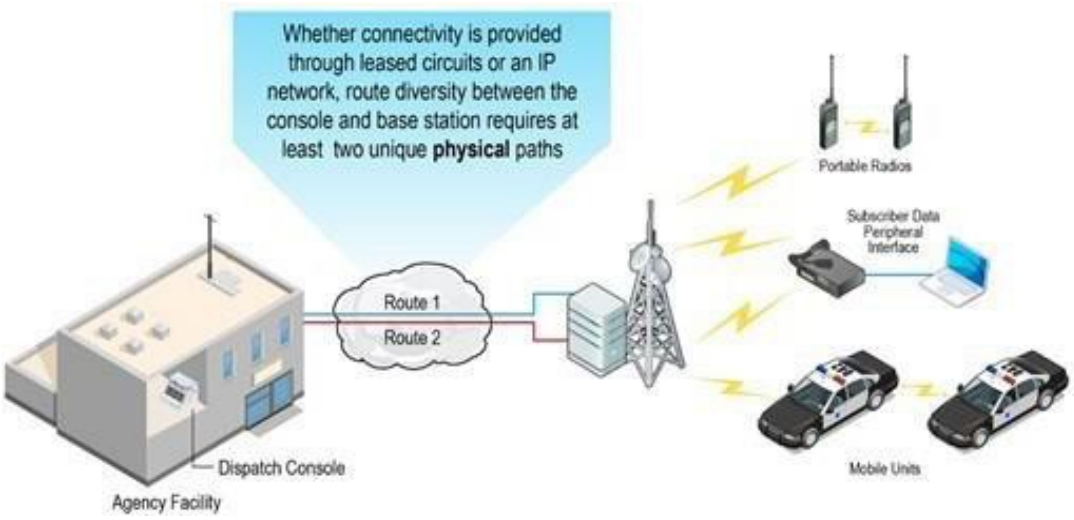

Figure 2: Route Diversity for a Land Mobile Radio Architecture

Though this document focuses only on communications network diversity, following Project 25 (P25) standards for LMR systems can improve resiliency. P25 standards encourage use of enhanced features,

capabilities, and services designed specifically for the rigors of the public safety environment. The standards articulate requirements for reliable software implementation, ruggedized hardware platforms, and systems design for high resiliency and redundancy.

3.0 COMMUNICATIONS RESILIENCY ASSESSMENT BENEFITS

Conducting a resiliency assessment of public safety telecommunication resources that enable and support mission-critical services ensures:

- Continuity of service in the event of an emergency
- Increased organizational control
- Prioritization of areas for network improvement
- Justification for network improvement funding requests
- Fulfillment of organizational diversity assessment requirements

4.0 DHS PUBLIC SAFETY RESILIENCY CAPABILITIES

CISA EDD has established tools and capabilities and maintains technical expertise from previous assessments to assist any public safety organization with its analysis. ECD focuses on the local access network because this area of the network typically has the least resilience, while urban and national networks tend to have more resilience. ECD's focus on public safety resilience extends beyond local access to address risks associated with infrastructure architecture, emerging technologies, and cybersecurity.

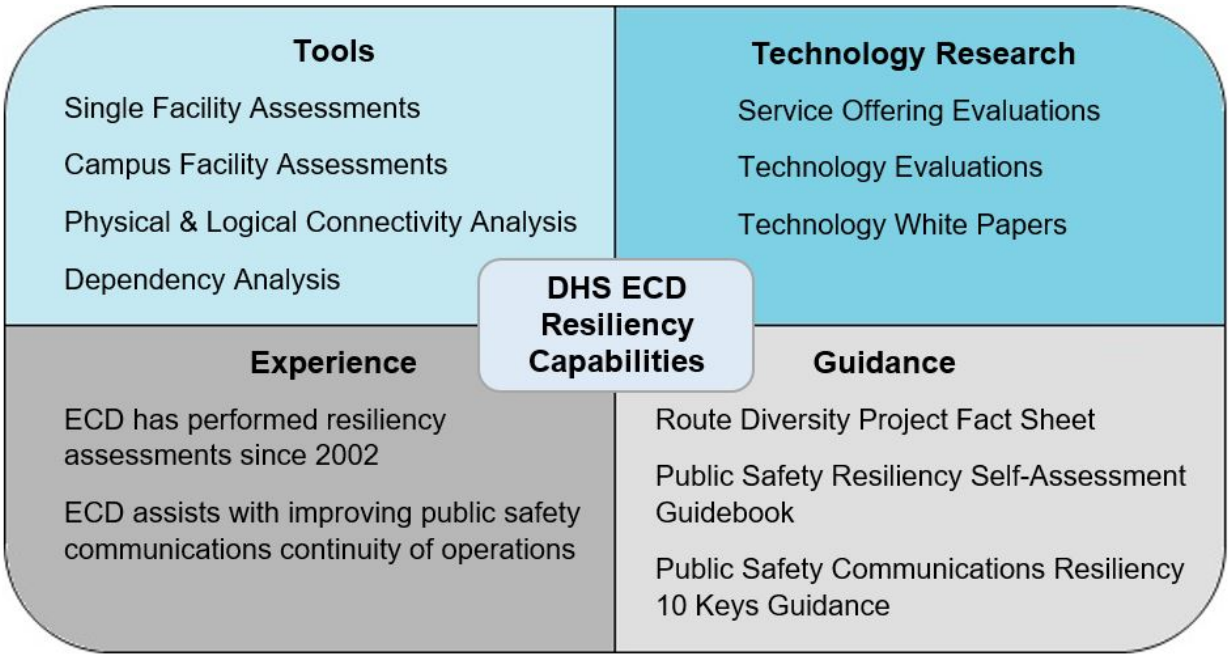

Figure 3. ECD Resiliency Capabilities

5.0 RESILIENCY ASSESSMENT METHODOLOGY

ECD has developed a three-step method for organizations to determine communication system connectivity, develop connectivity maps, and analyze diversity within their network and/or interconnected communications networks. Though this document focuses on the diversity component of resiliency, ECD has found that these assessments often uncover physical, operational, and cyber risks not associated with routing. In these instances, the risks are documented and ECD suggests using the full breadth of DHS risk mitigation tools and capabilities to develop solutions that improve overall resilience. DHS offers a collection of initiatives that can be applied to reduce communications and cyber risks, a sampling of which are shown in Appendix 1. Many of these efforts support federal, state and local users, as well as public and private critical infrastructure entities. In some instances, technical solutions may only apply to federal organizations, however the methodology in this document, as shown in Figure 4, can be applied to most networks and can provide cost savings in addition to reducing overall risk.

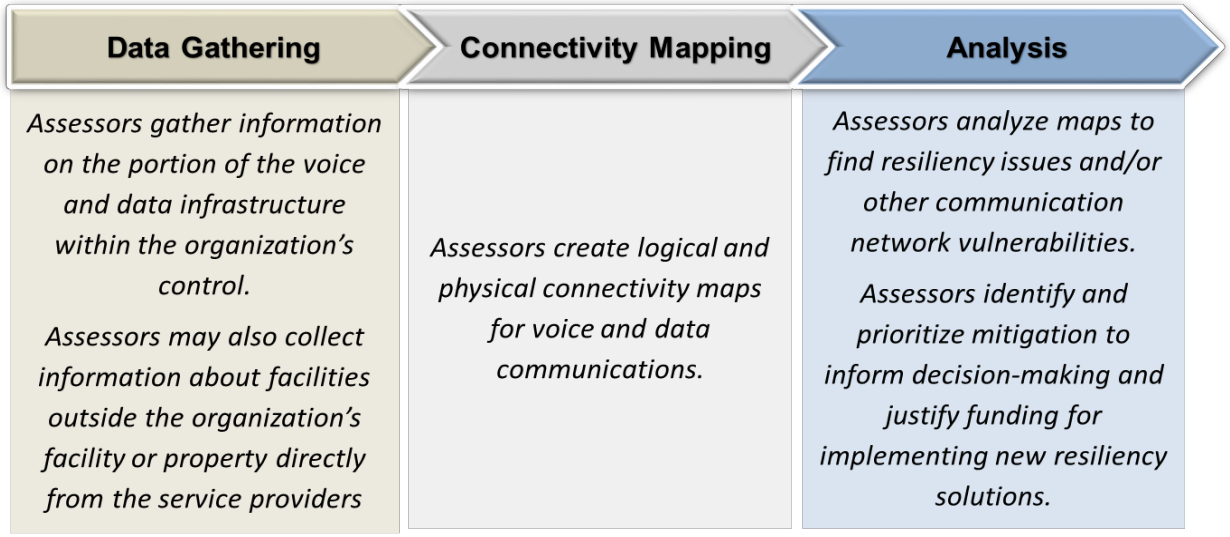

Figure 4. Basics of the Resiliency Assessment Methodology

ECD designed the methodology so that an organization's staff can evaluate their infrastructure in coordination with their service provider(s) to determine the routing of their voice and data communications. The methodology includes instructions for completing each step along with examples and sample results. All facility and carrier information presented in figures, text, and tables throughout this document is completely notional and provided to facilitate explanation.

The methodology is an assessment of only network assets up to and including the CO or point-of-presence (POP) for voice and data functions, respectively.[1] In addition, this assessment focuses on physical (Layer 1) network solutions[2]. This scope was chosen because:

- Layer 1 network solutions are most easily controlled and changeable by the organization
- Organizations have limited ability to control network assets or routing past the CO or POP
- Long distance voice and long-haul data carriers will likely have geographic diversity built into their network to protect it from all but the largest scale threats
- Local service providers' networks typically have fixed physical paths with static point-to-point connections, whereas long-haul networks have physical paths with dynamic routing that could create multiple connections

A facility may be served by two or more CO or POP sites. In fact, this is often an effective way to increase network resiliency. During an assessment, the organization should consider all CO or POP sites serving in the location of its facility.

5.1 Step 1: Data Gathering

In the data gathering phase, an organization first identifies the communication systems used to support its operations at the facility and collects relevant data on the connectivity of the systems.[3] Most of the information should be available internally. The organization should have information about the services used within the facility and procured communications services. Organizations may need to collect information about facilities that are a part of a service provider's network directly from the service provider to determine the routing of their voice and data communications. It is critical for the organization to collect and compile the most accurate information possible in Step 1 as it will be used to create logical network connectivity maps of the local voice and data communications network in Step 2 of the assessment process. Though not all information is readily available, ECD has demonstrated that unknown information does not preclude assessment. However, the more specific and accurate the data gathered, the easier it may be to implement the mitigations identified by the assessor.

---

[1] While this assessment focuses on networks up to and including the CO or POP, route diversity deficiencies may exist beyond that scope. For organizations interested in increasing route diversity beyond the CO or POP, enter "diversity" in the search criteria at the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) Best Practices website. https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data

[2] Layer 1 is described by the International Organization for Standardization (ISO) as the "physical" layer. This layer includes the electrical and physical specifications for data connections, the relationships between a given device and the medium over which it is connected (such as copper wire, fiber optic line, microwave signal, etc.), the transmission mode (such as simplex or duplex), and the topology of the network to which they are connected (such as mesh, ring, etc.). For more information, refer to the standard Open Systems Interconnection Model by ISO 7498-1 at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[3] The following assumptions are part of the best practices in this document regarding assessment:

- The organization's service providers will cooperate in supplying needed facility and link data.
- Information that is obtained from service providers is current as of the date it was obtained. However, service providers might subsequently modify connection paths or their facilities. In these cases, it cannot be assumed that service providers will automatically notify the organization unless it is part of a Service Level Agreement. It is the responsibility of the organization to verify the routes periodically with the service provider.
- Knowledgeable technical representatives familiar with the organization's communications systems will perform the assessment process.

Communication System Identification

The organization should begin its analysis by examining the communication systems it employs to support critical functions. The organization should examine its mission and primary mission-essential or critical business functions to establish a list of the communication systems and infrastructure that are necessary to perform those functions.

In most cases, the organization will identify separate voice and data communication systems. An organization can use one converged system or a next generation communication system that may utilize a combination of wireless and wireline networks for end-to-end connectivity.

The network assessment methodology presented in this document ends at the CO. However, the methodology could be extended to the inter-exchange carrier (IXC) or access tandem (AT). The organization's service provider should be able to supply the information. This information might be useful to determine whether two COs are using the same IXC or AT, thereby reducing the route diversity benefits of having connections to each.

Examples of potential organization communication systems include the following:

- Wireline voice networks
- Wireline data networks
- Wireline combined voice/data networks (VoIP)
- Wireless networks (e.g., cellular, microwave, WiFi, LMR)
- Satellite networks

Data Information Sources

The information an organization collects on its local voice and data communications network is used in Step 2 of the assessment process. The organization gathers information on the portion of the infrastructure within its control, such as:

- Voice network type (i.e., private branch exchange (PBX) or Centrex)
- Organization-controlled communications assets (for example, PBX or router)
- Redundant organization-controlled communications assets
- Current voice and data service providers
- Entry and exit points to the facility

Organizations can obtain this information from service level agreements (SLA), telecommunications and cable plant personnel, and organization technical communications documents, among other sources. Service provider bills can also provide information on these services. In most cases, the invoices will detail the circuit identification numbers and IP addresses that the carrier will need to determine routing. These bills, along with the organization's payment team, can be a key source for the baseline inventory.

Organizations can collect information about services outside the organization's facility or property directly from the service providers to determine how voice and data communications are routed. ECD

recommends that assessors collect all information from within an organization before contacting the carriers to increase the specificity and focus of data collected. Assessors can obtain this information from various groups within the carrier's organization, including the sales and engineering teams. Sales personnel have information based on the unique vendor-buyer relationship, and engineering personnel keep detailed records of network designs. Assessors should coordinate with the organization's account representative to gain access to the carrier's engineering or design team to gather information.

5.2 Step 2: Connectivity Mapping

The organization uses information collected in Step 1 to create connectivity maps for voice and data communications.[4] These maps should clearly depict the organization's infrastructure and facilitate an analysis of communications connectivity. There are two types of maps to create: logical and physical.

Logical Maps

Logical maps provide a high-level overview of the basic connections between the facility and its service provider's CO(s) or POP(s). Logical maps provide a good starting point for this assessment and can serve as a functional substitute if exact physical routing locations cannot be obtained. The maps should include the following nodes and logical links:

- Organization facility site
- PBX or other customer premise equipment
- CO locations
- POP locations
- Logical circuit links between sites

Figures 5 and 6 provide examples of voice and data logical maps.

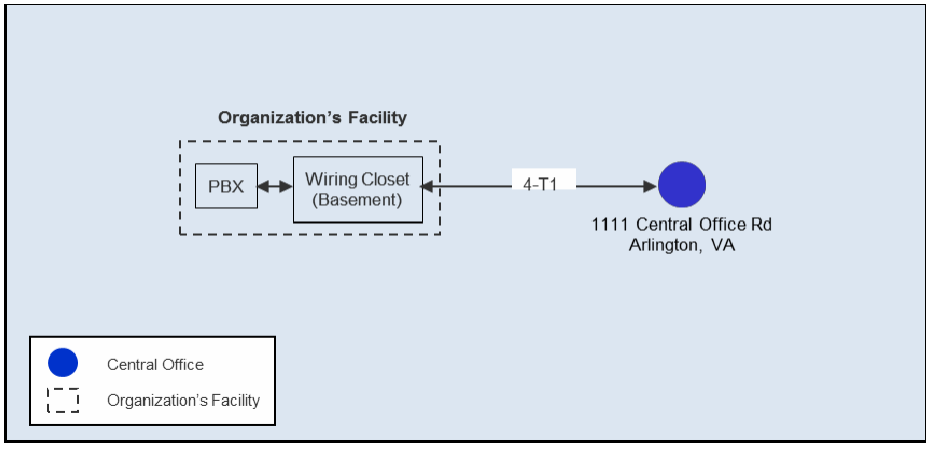

Figure 5. Sample Voice Logical Map with Single Entry Point

[4] The assessment is designed to be applied to a single facility. This methodology can be used for both government-owned and leased buildings; in other words, for any facility that serves a critical infrastructure function for both an emergency services organization as well as public safety services. Organizations with multiple buildings must perform the methodology for each building independently. For further information about a more in-depth methodology for assessing facilities with multiple buildings, please contact OEC@hq.dhs.gov.

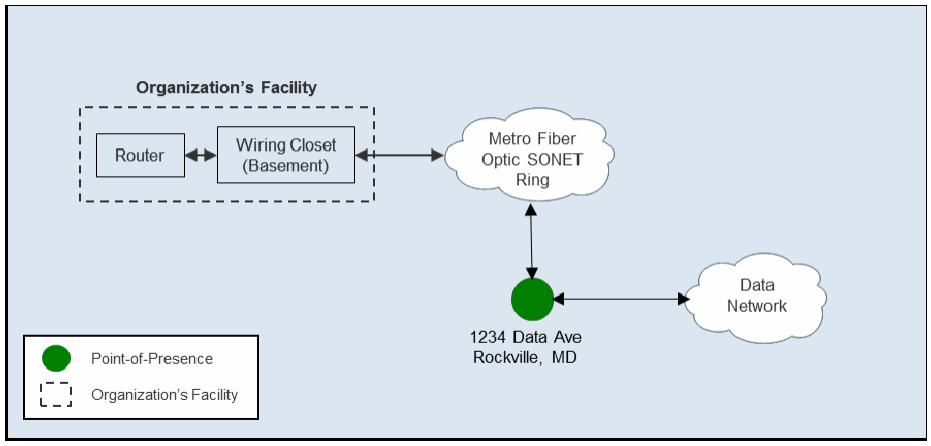

Figure 6. Sample Data Logical Map with Single Entry Point

Some facilities might have more than one connection to a CO or POP. The logical map of these connections will vary based network configuration. Figure 7 shows two connections that have different entry and exit points to the facility. Figure 8 shows a facility with two connections to a CO coming from one entry and exit point. The configuration in Figure 7 has a greater degree of diversity than Figure 8.

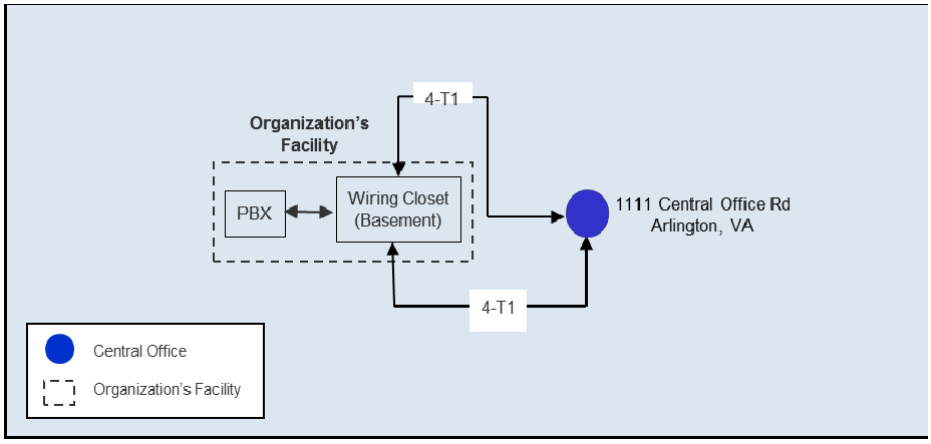

Figure 7. Sample Voice Logical Map with Two Connections and Two Entry/Exit Points

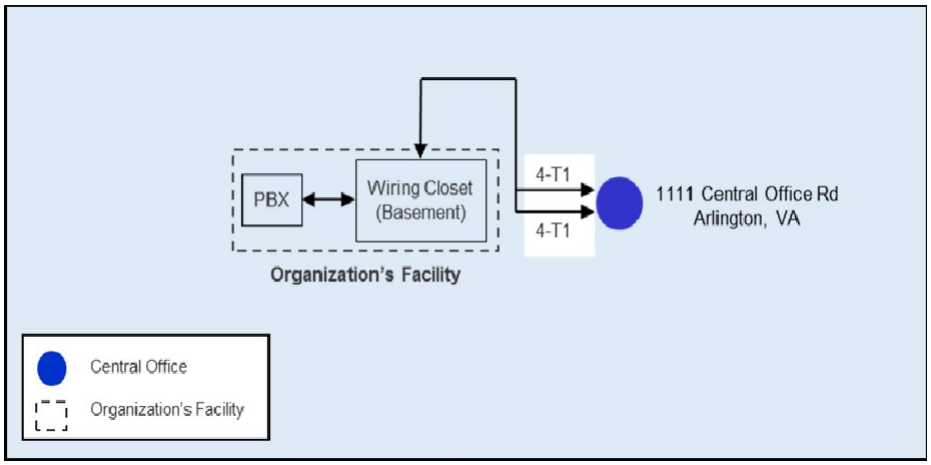

Figure 8. Sample Voice Logical Map with Two Connections and One Entry/Exit Point

Maps should be simple and accurate. Communications routes should clearly show the network facilities used to provide services. Assessors should also include facilities that provide secondary or backup services in the maps. To avoid confusion, organizations should indicate addresses on the maps to provide the exact location of the carrier's facilities.

Figure 9 depicts connections to separate COs using the same carrier. If multiple carriers provide service to the facility, each carrier's data should be included on the same logical map. Figure 10 demonstrates a facility using two voice carriers, Network Provider One (NP1) and Network Provider Two (NP2).

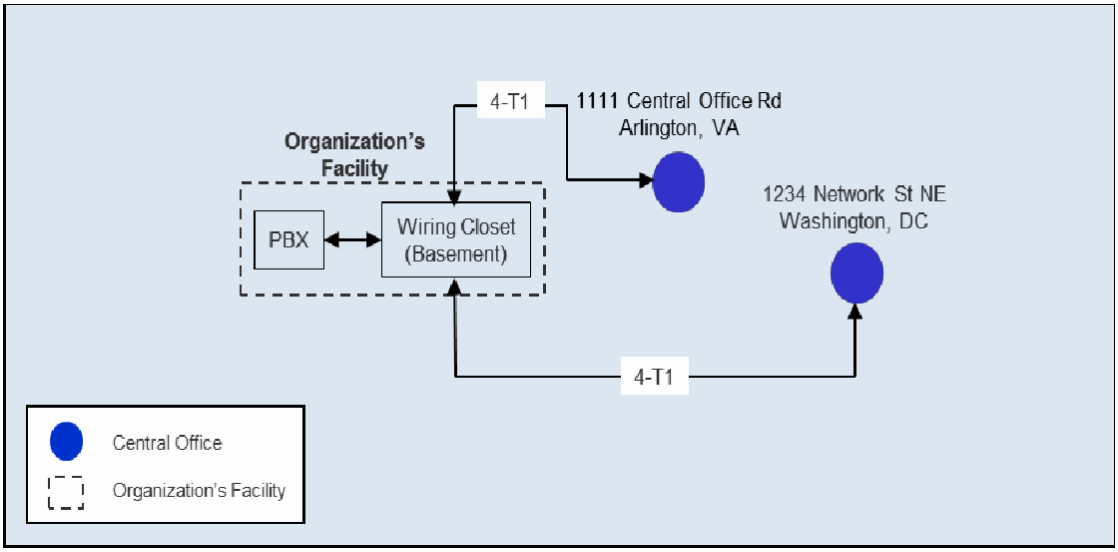

Figure 9. Sample Voice Logical Map with Connections to Separate COs

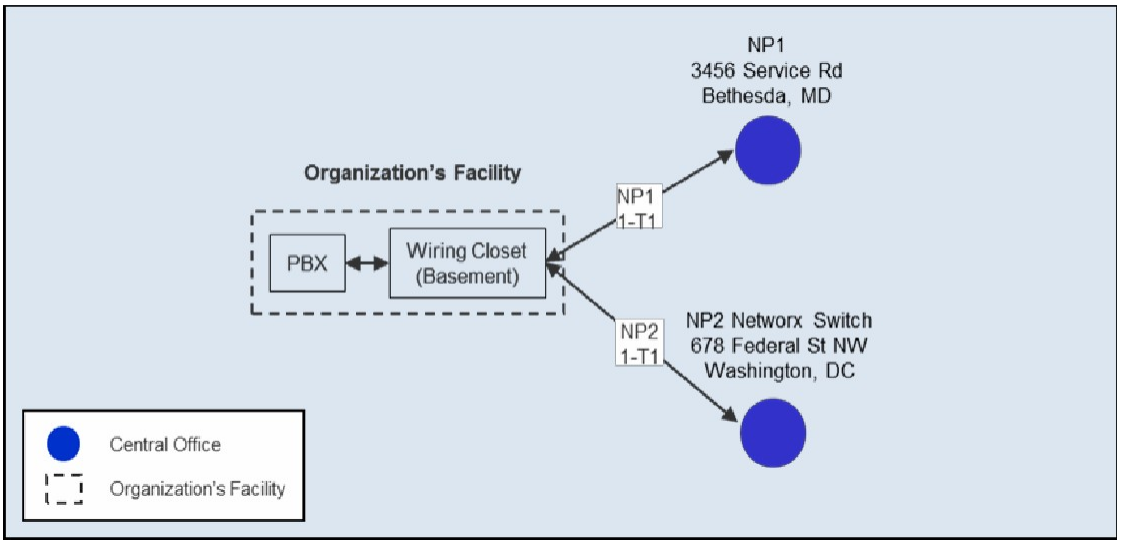

Figure 10. Sample Voice Logical Map with Multiple Carriers

The logical connectivity maps created for the local voice and data communications networks will be used in Step 3 of the assessment process to determine if route diversity exists in the organization network and to identify gaps.

Physical Maps

Physical maps display the exact physical route of a connection from the organization facility to its CO(s) or POP(s). Whereas logical maps can be helpful to provide high-level overviews, they may fail to detect underlying problems. For example, an organization might have services from two COs or POPs and might not be aware that the two connections follow the same path in some areas, as major rights-of-way are often shared by numerous service providers. By mapping the physical paths of each connection back to the CO or POP, the organization will have a better understanding of the actual degree of diversity that exists. Physical maps are also useful in the case of single points-of-failure because they allow the organization to develop more effective mitigation solutions. Knowing the path that a connection follows will allow the organization to select a mitigation solution that follows a different path.

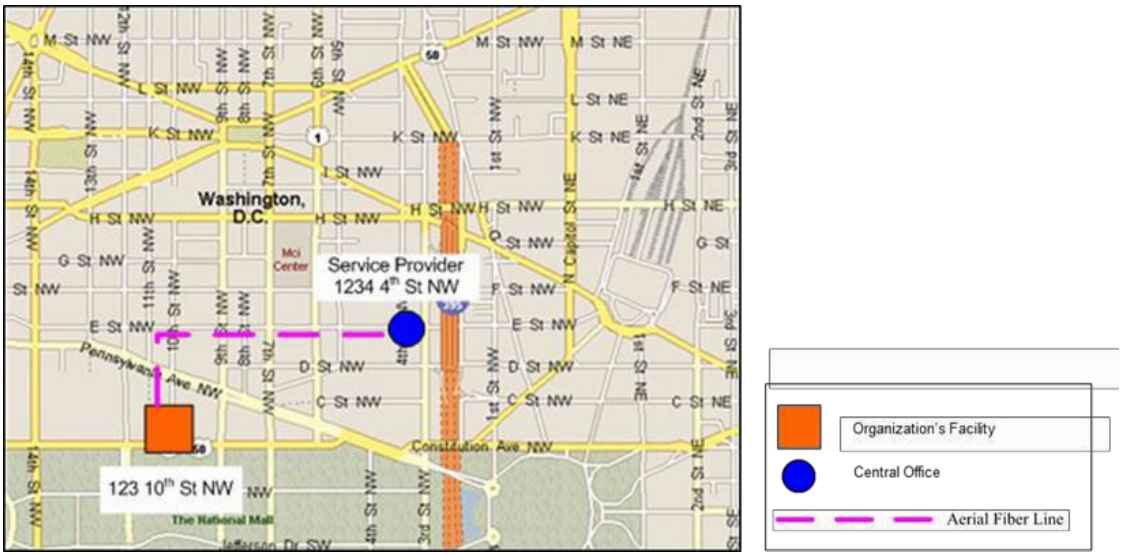

Figure 11. Sample Voice Physical Map

Figure 12. Sample Data Physical Map with Two POPs

There are several ways organizations can obtain information on exact physical connection paths. First, the organization can work with its service provider. Assessors can provide the circuit identification numbers and IP addresses to the provider, and the provider will likely be able to identify the path followed by a connection. However, a service provider may be unable or unwilling to provide this information. In that case, assessors may be able to get this information through the city municipal office where the organization is located. Municipalities maintain information about the location of utility routes within its jurisdiction. If communication paths are not part of these records, the municipality should be able to identify major rights-of-way, thereby allowing assessors to make informed estimates.

5.3 Step 3: Analysis

Once maps are created, an organization can analyze diversity within its network and/or interconnected networks. The maps are easily analyzed by understanding the common diversity issues associated with voice and data networks described below. The organization may use the analysis to pinpoint areas that lack diversity and, in turn, make appropriate decisions for implementing new resiliency solutions.

Common Communications Resiliency Deficiencies

This section describes five common resiliency deficiencies and mitigation strategies to aid organizations in determining whether or not there is sufficient resiliency present in their voice and data networks. Neither the list of deficiencies nor the list of solutions is exhaustive. Therefore, organizations should confer with their service providers to see what options exist for their own unique circumstances. Assessors compare the connectivity maps against these deficiencies and note any issues that exist.

- **Non-Redundant Organization Equipment**
  Communications equipment located within the organization's facility is vulnerable to failure. Loss of equipment may result from various issues including software failure, physical damage, hardware failure, and configuration errors. Communications will be completely impaired without operable equipment at the organization's facility until the equipment can be replaced or fixed. Organizations without backup or redundant equipment are at a higher risk of network disruption due to a lack of resiliency. Organizations can best determine the redundancy of their equipment on a logical map, as the equipment is most likely inside the facility. Redundant routers and PBX equipment will enable the organization's communications to remain in operation by reducing or eliminating downtime.

  Figure 13 on the following page demonstrates an example of equipment deficiency and Figure 14 shows the remedy through implementation of redundant equipment.

Figure 13 provides an example of a logical map showing a lack of redundant equipment.

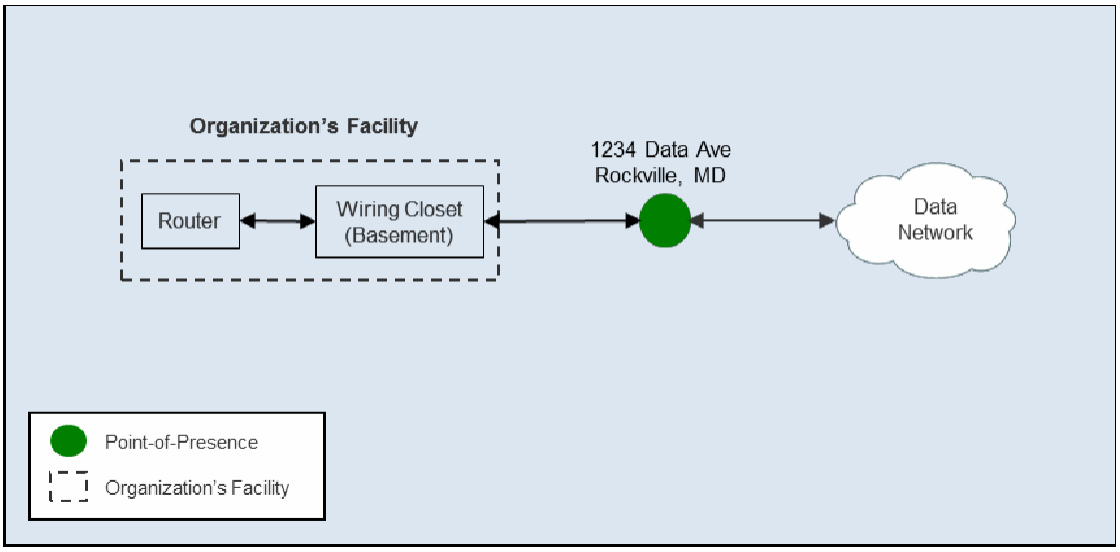

Figure 13. Non-Redundant Organization Equipment – Deficiency

Figure 14 shows an example of how to remedy the situation by implementing redundant equipment at the organization's facility. Note that the two routers are on separate floors. ECD recommends that organizations place redundant equipment on separate floors, if possible. This way, if one of the floors is damaged, the equipment on the other floor may remain operational.

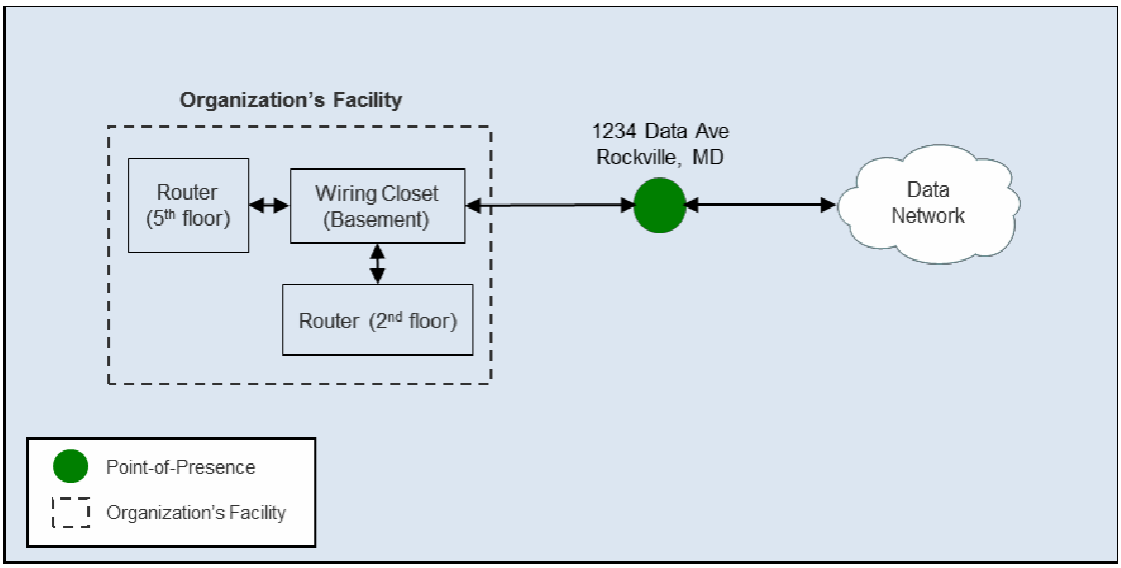

Figure 14. Non-Redundant Organization Equipment – Remedy

➢ **Single Point-of-Failure**

The most common resiliency issue occurs when an organization has a single line of service from a single service provider. The loss of any asset along the path from the organization facility to the CO or POP will cause a complete outage in communications service. This outage may result in prolonged downtime depending on the location and nature of the damage. Single points of failure are easily identifiable. Figure 15 provides an example configuration with a single point-of-failure.

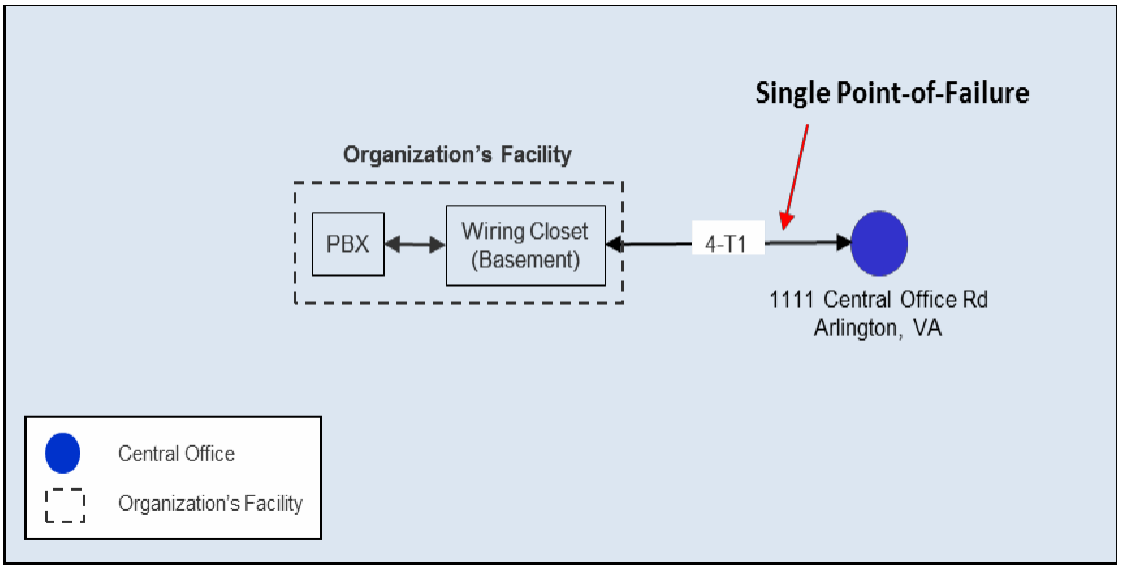

Figure 15. Single Point-of-Failure (Voice) Shown on a Logical Map

Single points-of-failure can be mitigated in several ways. The organization can:

- Add an additional, physically-separate connection to the CO
- Purchase back-up services from another service provider (ideally one that uses a separate CO)
- Purchase wireless services (such as microwave, WiFi, satellite phones) that can connect to an alternate CO

➢ **Common Carrier Facilities**

This resiliency issue occurs when two carriers provide service to an organization and use the same servicing CO (for voice) or POP facility (for data). An organization could procure services from separate carriers without knowing that physical assets within the two networks are shared. The loss of the common asset negates the advantages of separate carriers, as both networks will experience the outage. This problem is frequently found in backhaul and long-distance networks, as they often share local COs before transferring to their switches.

Carriers often share communications facilities to minimize the cost associated with building and maintaining their own assets. CO equipment, CO facilities, and POP facilities are examples of assets which are often shared amongst carriers. Therefore, organizations should collect the address information for each facility in the carriers' networks for analysis of logical connectivity maps. Although separate assets may be used, they could be located in the same building.

Figure 16 provides an example of two long-distance carriers that are dependent on the same local exchange carrier to provide access connectivity resulting in shared, common facilities regardless of different entry points into the organization facility and different long-distance networks to which they connect.

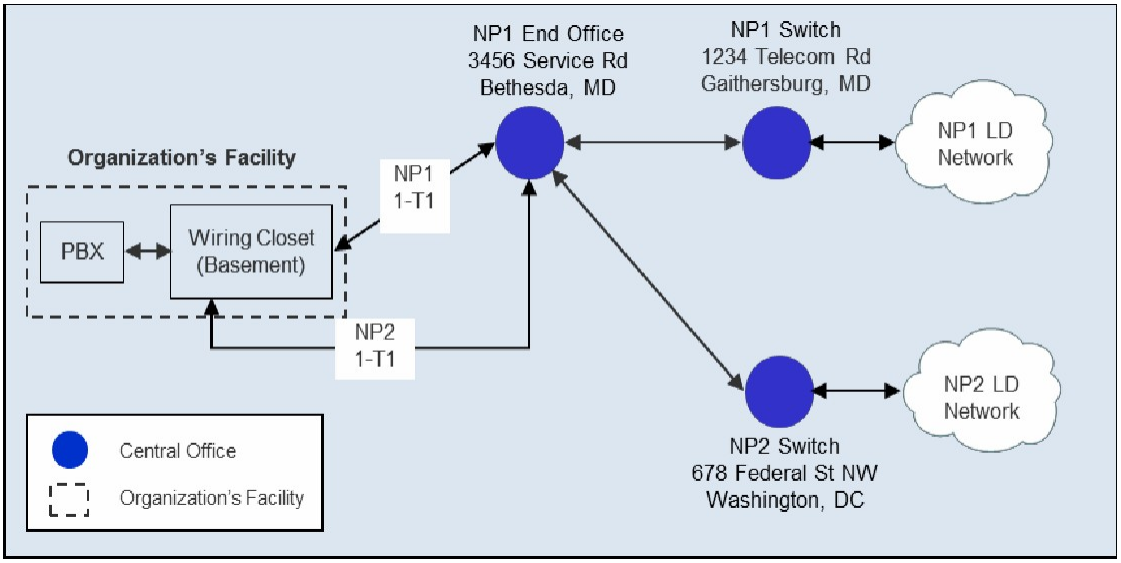

Figure 16. Common Carrier Facilities Displayed on a Logical Map

Figure 17 shows the same problem on a physical map. Note that the facility does have a degree of route diversity because it has two physically separate connections to the NP1 CO. However, the organization's resiliency could be improved if NP2 connected to a different CO; that way, if the primary CO was damaged, the secondary CO could still provide service to the organization. This is most likely the reason the organization purchased service from two providers in the first place, and the organization might not be aware of the problem until performing this assessment.

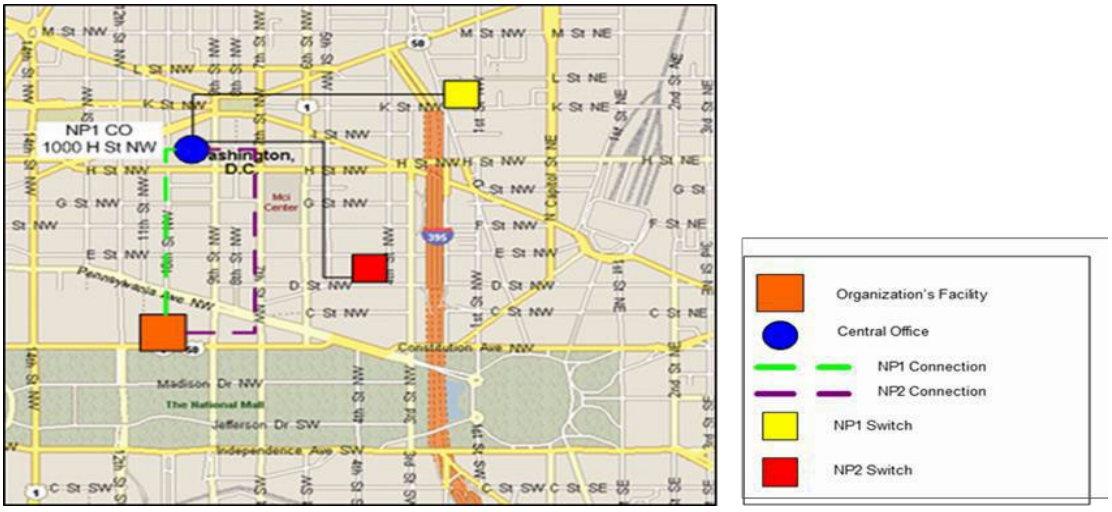

Figure 17. Common Carrier Facilities Shown on a Physical Map

Organizations can mitigate common carrier facilities deficiencies by requesting one of its carriers to use different facilities, or canceling service with one provider and purchasing services from a different provider that uses separate facilities.

- **Common Local Loop**

This resiliency issue occurs when two carriers provide service to the organization and use the same local loop connection to the organization's facility. Incumbent local exchange carriers are required by law to lease the local loop connection for competing local carriers to provide services. Therefore, an organization could have procured services from separate carriers, unaware that transmission paths for the two networks are shared. Threats to the common loop connection negate the advantages of separate carriers, as both networks will be vulnerable to the same potential single point-of-failure.

The common local loop is also one of the most difficult issues to identify because it involves comparing information from two carriers and it could involve separate fibers in the same conduit. One way to recognize the potential for a common local loop is checking the entry and exit points at the organization's facility. Organization facilities with multiple carriers and only a single entry/exit point at their facility will likely have this type of resiliency issue.

Another way to recognize this issue is to compare the CO addresses. If the two carriers share the same CO, then there is a high likelihood, they use the same routing. Figure 18 shows a typical logical map with a likely common local loop issue.

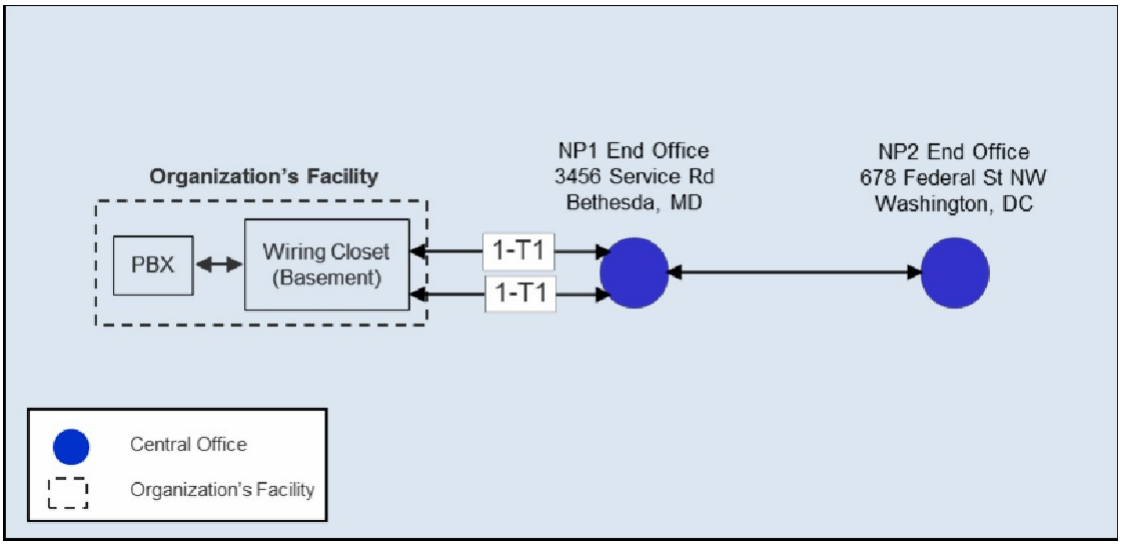

Figure 18. Common Local Loop Shown on a Logical Map

Figure 19 shows the same problem on a physical map.

Figure 19. Common Local Loop Shown on a Physical Map

Organizations can mitigate common local loop deficiencies using the same methods for common carrier facilities deficiencies—requesting one of its carriers use a different facility, or canceling service with one-provider and purchasing services from a different provider with separate facilities.

- **Common Physical Paths**

  Communications service providers often use major rights-of-way (for example, roads, bridges, railroads) and the same conduits (for example, ducts, pipes, etc.) in the routing paths of their connections to customers' facilities. An organization might purchase service from two service providers, verify that the service providers use different COs or POPs, and still face this problem. An organization with only one entry and exit point in its facility is more likely to have this problem. Organizations can only detect this problem on a physical map. Figure 20 shows this problem for an organization facility with one entry/exit point in its facility.

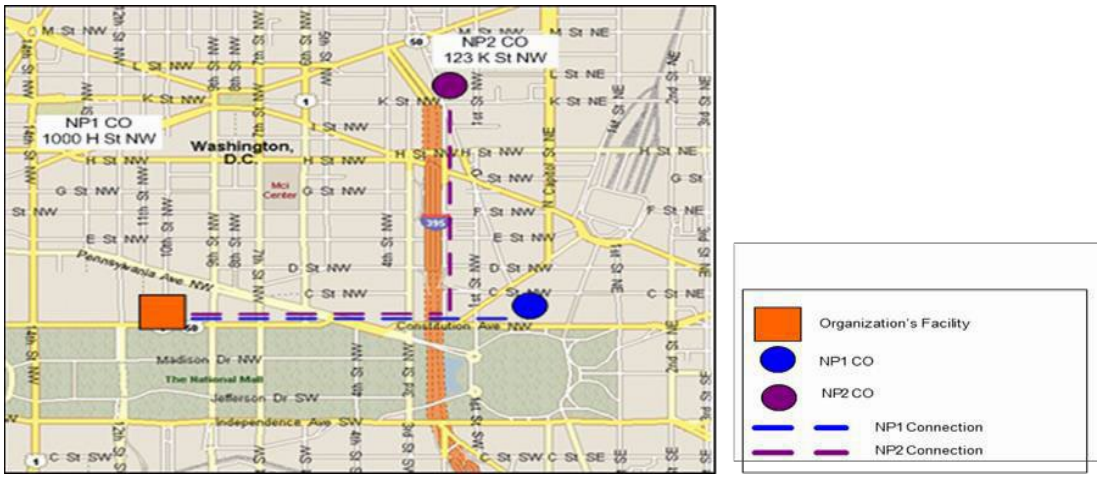

Figure 20. Common Physical Path

Common physical paths might be more difficult to mitigate, as some locations mat not have any other physical paths besides major rights-of-way. However, there are some options:

- The organization can purchase back-up wireless services (such as satellite phones or WiFi) or can establish a wireless link (for example, microwave) between its facilities
- The organization can request one of its service providers establish a different, physically separate connection to its CO, although cost implications of this option are typically high, especially in rural areas
- The organization can add an additional, physically separate entry and exit point to its facility (if it currently has only one) and route one of its connections through that new point

6.0 COMMUNICATIONS RESILIENCY MITIGATION SOLUTIONS

Once the network evaluation has been conducted, the organization will have documented key factors contributing to its network resiliency status. If resiliency issues are uncovered, the organization must determine how these issues impact its mission and when to address these deficiencies. ECD recommends that organizations evaluate all solutions for areas lacking resiliency. An organization should select the appropriate solution based on its priorities, budget, and other internal factors.

Certain solutions will be better suited for some organizations than others. For example, leased dark fiber is a common solution that provides alternative communications physically separate from existing circuits, but the cost is relatively high. Some organizations may determine that dark fiber leasing is not cost-effective. Alternatively, microwave and WiFi are two solutions that provide wireless connectivity. The cost associated with these solutions is relatively low compared to a physically separate wireline connection, but the implementation of these solutions in a facility may be difficult. With respect to a microwave solution, the tower cost and maintenance can present challenges, and range and attenuation can be problematic depending on the topography and atmospheric conditions of the facility's location.

6.1 Important Note About ECD Priority Telecommunication Services

ECD provides several priority telecommunication service programs for organizations in critical sectors to ensure the survivability and recovery of communications infrastructure. Organizations should determine whether they participate in any of the following programs:

- Government Emergency Telecommunications Service (GETS) – GETS provides emergency access and priority processing in the local and long-distance segments of the public switched network. Public and private organizations use GETS in crisis situations when the network is congested and the probability of completing a call over normal or another alternate telecommunication means has significantly decreased.[5]

[5] Additional information can be found at http://www.dhs.gov/gets.

- Wireless Priority Service (WPS) – WPS provides priority for calls made from cellular telephones by emergency personnel during crisis situations when cellular networks can experience congestion due to increased call volumes or damage to network facilities.[6]
- Telecommunications Service Priority (TSP) – TSP provides national security and emergency preparedness (NS/EP) users priority provisioning and restoration of telecommunications services that are vital to coordinating and responding to crises.[7]

7.0 CONCLUSION

Government and public safety entities rely on voice and data communications networks to achieve their missions. Increasing a facility's resilience will only help ensure greater communications continuity during emergency situations. Admittedly, it is difficult for an organization to achieve full end-to-end resilience, as the organization may have little control over communications routing past the CO. However, an organization can greatly improve "always available" communications by identifying and mitigating potential issues through a self-assessment (such as the one presented in this document) of its local access network.

Performing a self-assessment and addressing issues identified enables:

- Continuity of service in the event of an emergency
- Increased organizational control
- Prioritization of areas for network improvement
- Justification for network improvement funding requests
- Fulfillment of organizational diversity assessment requirements

Communications resiliency is an important aspect of an organization's mission-critical operations. Network redundancy and diversity can help organizations continue to function properly in emergency situations. Organizations must ensure that their networks are resilient in order to maintain operations and fulfill their missions. ECD is available to provide assistance to organizations throughout the process of improving network resiliency.

For additional information on public safety communications resiliency, please contact ECD at OEC@hq.dhs.gov.

[6] Additional information can be found at http://www.dhs.gov/wps.
[7] Additional information can be found at http://www.dhs.gov/tsp.

APPENDIX 1: DHS Network Risk Mitigation Initiatives

Though this document focuses on the diversity component of public safety communications resiliency, ECD has found that these assessments often uncover physical, operational, and cyber risks not associated with routing. In these instances, the risks are documented and ECD recommends investigating solutions including the full breadth of DHS risk mitigation tools and capabilities. DHS offers a collection of programs and initiatives that can be applied to reduce cyber risks, a sampling of which are shown in the table below. Many of these efforts support missions that cover federal, state and local users, as well as public and private critical infrastructure entities. In some instances, technical solutions may only apply to federal organizations, however the methodology can be applied to most networks and can provide cost savings in addition to reducing cyber risk.

DHS Network Risk Mitigation Initiatives (Non-Comprehensive)	
Telecommunications Service Priority (TSP)	Authorizes critical government, emergency preparedness, and public safety organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. (www.dhs.gov/tsp)
Government Emergency Telecommunications Service (GETS)	Provides critical government, emergency preparedness, and public safety personnel priority access and prioritized processing in the local and long-distance segments of the landline networks, greatly increasing the probability of call completion. (www.dhs.gov/gets)
Wireless Priority Service (WPS)	Provides critical government, emergency preparedness, and public safety personnel priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion. (www.dhs.gov/wps)
Network Flow Collection	Provides the enterprise with an awareness of the type and volume of traffic flowing into (and out of) the enterprise network. Information includes source/destination IP address, domains, and ports. This data can be filtered and searched to identify anomalous flow patterns, and initiate further research into potential risks and attacks. (www.dhs.gov/einstein)
Intrusion Detection (IDS)	Provides IDS sensors and develops digital signatures which are loaded into the IDS to identify threats. Organizations receiving this service are able to view alerts created by the IDS (occurring when signatures identify pattern matches in network traffic). (www.dhs.gov/einstein)
Intrusion Prevention (IPS)	Deploys IPS to public and private network owners. IPS is like IDS in that digital signatures are used at the sensor. With IPS, when signatures identify pattern matches, countermeasure actions are taken such as dropping or rerouting traffic. While network flow collection and IDS are passive (monitoring and alerting) cybersecurity measures, IPS is an active security measure. (www.dhs.gov/einstein)
Risk Assessment and Risk Analysis	Provides infrastructure baseline assessments, vulnerability assessments, impact assessments, and comprehensive risk and mitigation analyses of public safety infrastructure and services. Another recommended resource for risk assessment is the National Institute of Standards and Technology (NIST) Cybersecurity Framework. (https://www.nist.gov/cyberframework)

APPENDIX 2: GLOSSARY

Assessment. The process of acquiring, collecting, processing, examining, analyzing, evaluating, monitoring, and interpreting the data, information, evidence, objects, measurements, images, and sound, among others, whether tangible or intangible, to provide a basis for decision-making.

Central Office. Central Office (CO) is a physical facility housing one or more end offices.

Common Carrier Facility. A place at which two or more carriers utilize the same servicing Central Office (for voice) or Point of Presence facility (for data).

Common Local Loop. A condition that exists when transmission paths for two or more carrier networks are shared.

Continuity of Communications. The ability of critical government and emergency response agencies to maintain communications capabilities when the primary infrastructure is damaged or destroyed.

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: *2013 National Infrastructure Protection Plan*)

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 9-1-1 communications systems and control systems. (Source: *2013 National Infrastructure Protection Plan*)

End Office. End Office (EO) is the switch that provides a customer dial tone and local telecom services.

Inter-Exchange Carrier. Inter-Exchange Carrier is a service provider of inter-local access transport area (LATA) or long distance services between LATAs on an intrastate or interstate basis.

Interoperability. Ability of emergency responders to communicate among jurisdictions, disciplines, frequency bands, and levels of government as needed and as authorized. System operability is required for system interoperability.

Land Mobile Radio (LMR) Systems. Terrestrially-based wireless narrowband communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works companies, and even the military to support voice and low-speed data communications.

Non-Redundant Equipment. Key telecommunications/networking resources, including components or systems (hardware or software) that are not backed by redundancy.

Point of Presence. Point of Presence (POP) is the physical location where an inter-exchange carrier's circuits interconnect with the local lines of telephone companies.

Public Safety Answering Point (PSAP). A facility that has been designated to receive 9-1-1 calls and route them to emergency services personnel. A PSAP may act as a dispatch center. Public Safety Answering Point is often used with the term Public Safety Communications Center. (Source: *Communications Act of 1934*, as amended)

Reliability. Achieved in public safety land mobile radio systems through equipment redundancy and minimizing single points of failures through careful system design. System operators stock spare parts and, in some cases, transportable backup systems to restore system failures that do occur. Reliability must be considered at the earliest stages of system design.

Redundancy. Additional or alternate systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Route Diversity. Communications routing between two points over more than one physical path with no points in common.

Single Point-of-Failure. A key dependency, such as a single line of service from a single service provider, or other single source of componentry or connectivity which, if lost or damaged, could result in a system failure

Tandem. Tandems are switches that distribute calls between end offices. There are two types of tandems, access and local. Access Tandems (AT) switch long distance toll calls. Local Tandems (LT) switch local toll calls between end offices in the same Local Access Transport Area (LATA).

APPENDIX 3: ACRONYMS

AT	Access tandem
CO	Central Office
DHS	Department of Homeland Security
EO	End Office
ECD	Emergency Communications Division
EOC	Emergency Operations Centers
GETS	Government Emergency Telecommunications Service
IDS	Intrusion Detection
IP	Internet Protocol
IPS	Intrusion Prevention
ISO	International Organization for Standardization
IXC	Inter-exchange carrier
NP1	Network Provider One
NP2	Network Provider Two
LATA	Local Access Transport Area
LT	Local Tandems
P25	Project 25
PBX	Private Branch Exchange
POP	Point-of-presence
PSAP	Public Safety Answering Points
PSCC	Public Safety Communications Centers
SLA	Service Level Agreements
TSP	Telecommunications Service Priority
VoIP	Voice/data networks
WPS	Wireless Priority Services