TLP: WHITE

RISK TO CRITICAL INFRASTRUCTURE: TELECOMMUNICATIONS CENTRAL OFFICES

Central offices are essential hubs within the U.S. telecommunication infrastructure. A disruption at a central office could impact nearby critical infrastructure operations and disrupt communications within a geological region. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed this infographic to facilitate dialogue to improve telecommunications resiliency between service providers and their customers in critical infrastructure and federal, state, local, tribal, and territorial (FSLTT) governments.

RISKS TO CENTRAL OFFICES

1 Physical
Physical risks, such as human-made or natural events, can impact equipment, personnel, and the operation of central offices and any interdependent systems.

2 Cyber
A compromise of systems in a central office could enable a cyber actor to impact the confidentiality, integrity, and availability of data that travels through the central office and move to other parts of the network.

3 Utilities and Services
Loss of critical infrastructure services could cause central office components to shut down due to power loss, or overheat from the lack of cooling systems.

4 Network Resiliency
A service interruption within a central office can cause full or partial communication outages within a region, and may lead to cascading disruptions to critical infrastructure operators until functionality is restored.

Risk Solutions Segments

1

Physical
Redundant systems, back-ups, physical security (including standoff distance), and a proper geographic location that enables the alternate routing of network traffic can mitigate risk.

2

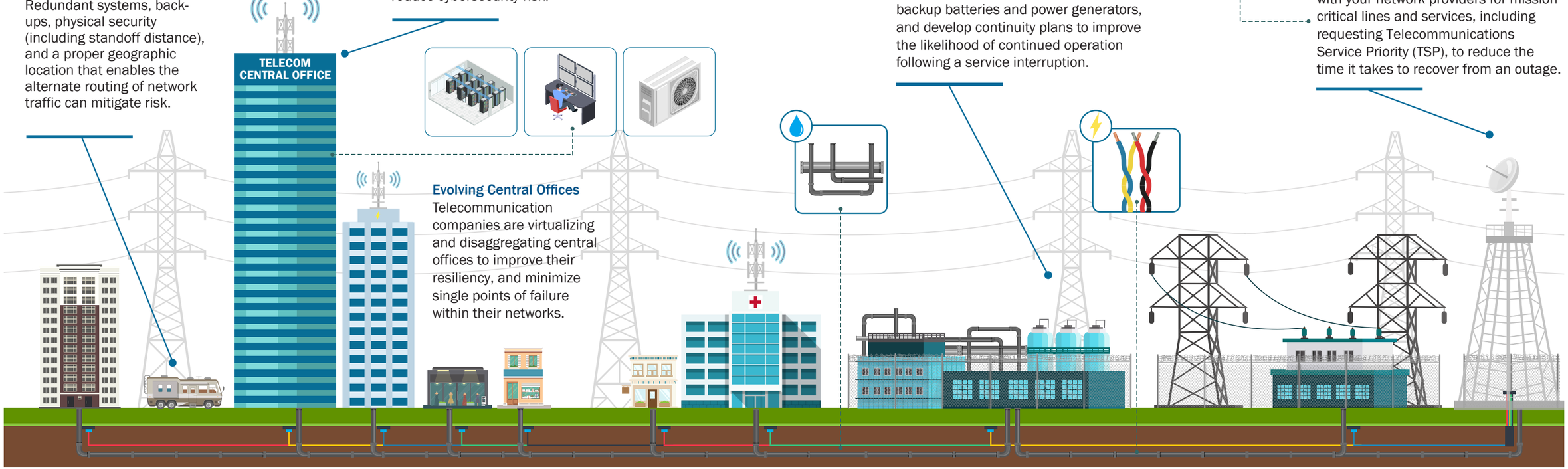
Cyber
Avoid the use of hardware or software from untrusted entities, utilize a cyber risk framework, and take proper cybersecurity measures to significantly reduce cybersecurity risk.

3

Utilities and Services
Identify utilities and services that a facility requires to successfully function, utilize backup batteries and power generators, and develop continuity plans to improve the likelihood of continued operation following a service interruption.

4

Network Resiliency
Verify physical diversity and redundancy with your network providers for mission critical lines and services, including requesting Telecommunications Service Priority (TSP), to reduce the time it takes to recover from an outage.



Evolving Central Offices
Telecommunication companies are virtualizing and disaggregating central offices to improve their resiliency, and minimize single points of failure within their networks.

Additional Resources: Telecommunications service providers, critical infrastructure, and FSLTTs can take steps to lower the risk to their facilities from physical and cyber threats. The **Statewide Interoperability Coordinators** can help service providers gain insight into states' strategic vision for interoperability, and assist in facilitating communications among responders during emergencies. Additionally, all stakeholders are encouraged to review the **National Emergency Communications Plan**, which establishes a shared vision for emergency communications and can facilitate conversations between providers and FSLTT to plan for, coordinate, invest in, provide services in support of, and use operable and interoperable communications to include Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and TSP for response and recovery operations. **CISA's Cyber Essentials Toolkit** is a guide for smaller organizations to develop an actionable understanding of where and how to start implementing organizational cybersecurity practices. For more information, email central@cisa.gov.

TLP: WHITE