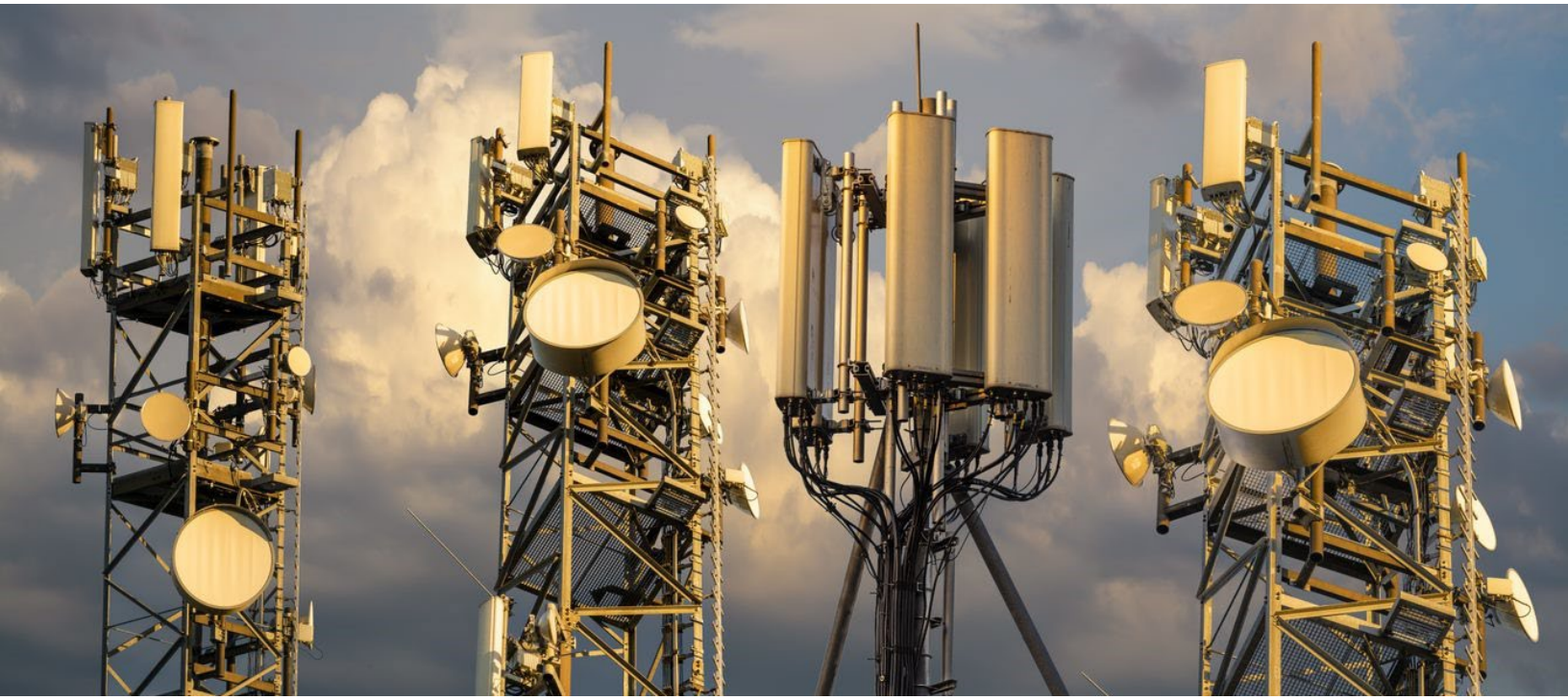
SAFECOM®

NCSWIC®



PUBLIC SAFETY COMMUNICATIONS DEPENDENCIES ON NON-AGENCY INFRASTRUCTURE AND SERVICES

Revised August 2024

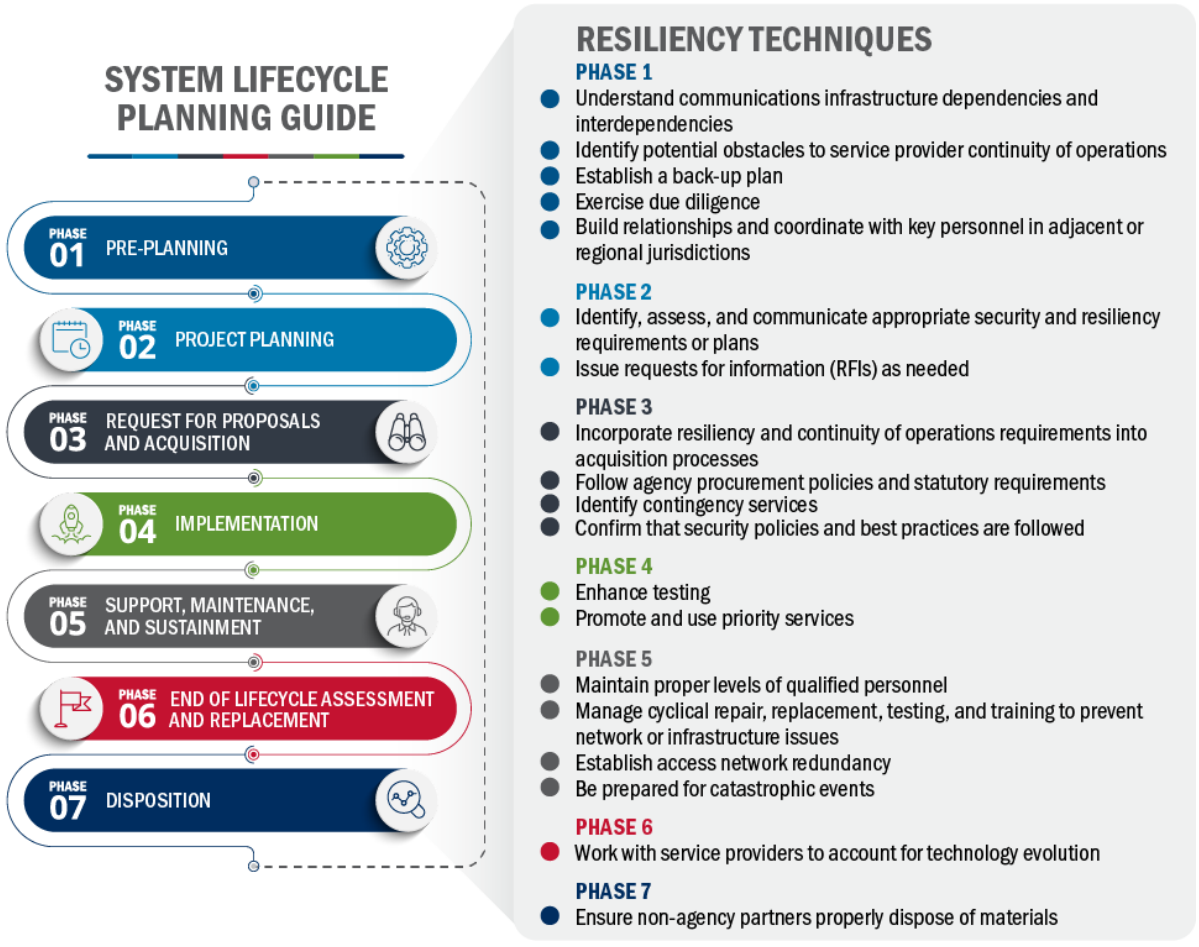
SAFECOM-National Council of Statewide Interoperability Coordinators

EXECUTIVE SUMMARY

Given the complexity of public safety communications systems and modern supply chains contributing to those systems, many public safety agencies find themselves relying on outside sources—commercial vendors and carriers, external agencies or departments, suppliers, and other organizations—to provide infrastructure and services. This collaboration between agencies sponsoring or owning the public safety communications systems and the external entities providing infrastructure or services comes with its own challenges, complexities, and opportunities.

To address public safety dependencies on non-agency communications infrastructure and services, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) developed this white paper to provide high-level insights for system administrators, public administration decision makers, and other stakeholders involved in public safety communications planning or implementation. While not a comprehensive guide, this document is intended to equip stakeholders with examples of real-world impacts of these dependencies, recommendations for ensuring resiliency and continuity of operations, and supplemental materials providing enhanced details about the various forms of dependencies and potential considerations and practices, including definitions of relevant acquisition, legal, and service-level documentation.

Recommendations have been provided using the "System Lifecycle Planning Guide" phases:



Throughout all lifecycle phases, greater collaboration between stakeholders is encouraged to ensure partners are mutually engaged in continuity of operations planning, governance processes, and adoption of cybersecurity and infrastructure security best practices. In addition, agencies will need to anticipate and prepare for the unexpected**.** Agencies should continually ensure steps are taken throughout the lifecycle to prepare for any and all types of disruptions, including changes in regulations, where third parties may be involved or may need to become involved, as public safety communications must operate under a variety of circumstances to ensure protection of life and property.

Supplemental information—definitions of access networks, use cases for various dependencies, definitions of procurement, legal, and other system documentation—is included as appendices to the main document.

Table of Contents

INTRODUCTION

Communications systems—the keystone of public safety operations—are vulnerable to natural disasters, human error, and physical and cybersecurity incidents. Communications systems owned and operated by public safety or emergency management agencies are typically built with enhanced resiliency and continuity of operations requirements. Even so, these systems are increasingly interconnected to non-agency owned and operated infrastructure components and services to send and receive emergency communications. According to the SAFECOM Nationwide Survey, **failure of equipment outside of the organization's control impacted 58 percent of respondents' ability to communicate.**[1] As such, SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) collaborated to develop this white paper to describe these Communications Sector components, highlight specific network outages that have impacted emergency communications, and detail ways to minimize dependency-related risks throughout the lifecycle of an emergency communications system.

The purpose of this white paper is to help system administrators, public administration decision makers, and other stakeholders involved in public safety communications identify non-agency dependencies that should be considered during system lifecycle planning and implementation.

WHERE HAVE THESE DEPENDENCIES BEEN REALIZED?

Emergency communications systems can depend on infrastructure or services from various sources outside the agency, from commercial vendors and contractors to government components in an outside jurisdiction (such as another local, state, or federal entity). These third-party entities can provide or host a range of components and services. Table 1 lists several examples of common components and services being deployed by public safety agencies (additional information for each system type can be found in Appendix B, C, D, and E, respectively).

Table 1. Real-World Impact of Dependencies

System	Service Outage Case Study
911	In early 2017, a carrier experienced 911 service outages on the company's Voice over Long-Term Evolution (VoLTE) network due to incidental interference from network updates. In less than an hour, about 2,600 911 calls failed. A Federal Communications Commission (FCC) investigation later stated that the carrier "failed to quickly, clearly, and fully notify all affected 911 call centers."[2] See Appendix B for additional details.
Land Mobile Radio	In the aftermath of Hurricane Florence in 2018, a local LMR system in North Carolina experienced disruption, leading to public safety responders critically relying on a broadband network during response. Given that the LMR system was the primary source of emergency communications, the broadband service in multiple instances provided the primary means of communications.[3] See Appendix C for additional details.
Broadband	During Hurricanes Irma and Maria, the Federal Emergency Management Agency (FEMA) deployed teams across Puerto Rico to register survivors for disaster assistance and conduct case inquiries. However, severely limited mobile broadband communications disrupted these efforts, leading to inaccuracies and significant delays as team members were forced to use offline solutions.[4] See Appendix D for additional details.
Cloud	Disruptions to one provider's cloud services in 2019 resulted in reductions to regional network capacity and a delay in search query response time. The service disruptions were caused by configuration changes to servers in a single region that incorrectly extended to neighboring regions.[5] See Appendix E for additional details.

[1] Cybersecurity and Infrastructure Security Agency (CISA), 2024.
[2] FCC, "FCC Settles Investigation into Two AT&T Mobility 9-1-1 Outages in 2017," June 28, 2018.
[3] Donny Jackson, "North Carolina city relies on FirstNet voice, data communications during Hurricane Florence," Urgent Communications, September 26, 2018, last accessed September 3, 2020.
[4] See Key Finding #13 in FEMA's 2017 Hurricane Season FEMA After-Action Report
[5] Benjamin Sloss, "An update on Sunday's Service Disruption," June 3, 2019, last accessed September 3, 2020.

HOW CAN AGENCIES AND SERVICE PROVIDERS IMPROVE COMMUNICATIONS RESILIENCY AND CONTINUITY OF OPERATIONS?

In today's complex and interconnected communications and information technology (IT) environment, non-agency infrastructure and service dependencies can take many forms and impact multiple agency and non-agency components responsible for maintaining communications systems and ensuring continuity of operations. Additional information about Communications Sector components may be found in Appendix A.

Due to the complexities of the Communications Sector, this document does not attempt to provide a comprehensive list of known non-agency dependencies for public safety communications and IT systems. However, several stakeholder-driven recommendations are provided to benefit agencies with dependencies on either infrastructure or services (or both). These recommendations are presented using the lifecycle framework as articulated by the Cybersecurity and Infrastructure Security Agency (CISA) in coordination with SAFECOM and NCSWIC in the *Emergency Communications System Lifecycle Planning Guide.*[6]

By approaching dependencies in the context of system lifecycle planning, agencies can be appropriately prepared before, during, and after any service-disruptive event. Following the lifecycle phases of the "System Lifecycle Planning Guide" (Figure 1), the recommendations in the following section, while not intended to be exhaustive, can provide a starting point for agencies to assess, anticipate, and address challenges to system continuity or resiliency.

Additionally, several ongoing activities that might be conducted throughout the lifecycle are provided. For example, activities such as engaging stakeholders and service providers, as well as coordinating with adjacent jurisdictions and state or territorial and federal partners, can have valuable impacts when encountering service-disruptive events.

Figure 1. System Lifecyle Planning Guide

[6] CISA, "Emergency Communications System Lifecycle Planning Guide," 2018.

PHASE 01 PRE-PLANNING

The pre-planning lifecycle phase may occur intentionally or organically as the agency assesses the current state of the communications system and its requirements. The agency may use this time to inform any decisions regarding replacing, upgrading, maintaining, acquiring, or implementing a communications system or system components.

During pre-planning, agencies might engage in the following recommendations:

- **Understand communications infrastructure dependencies and interdependencies.** In some cases, widespread network outages can result from a single node failure (e.g., a cut fiber or a cybersecurity incident). Drawing on existing resources to understand where these vulnerabilities exist within non-agency infrastructure enables partners to increase resiliency in the face of infrastructure damage, outages, or cybersecurity incidents
- **Identify potential obstacles to service provider continuity of operations.** Public safety agencies may work to identify possible obstacles service providers may face, which could impact their ability to fulfill their contractual obligations (e.g., roads becoming washed out following a disaster, limiting access to utility sites, power, and fuel/propane). In some instances, mitigation may require service providers working with other service providers to resolve the circumstances (e.g., the utility company working with local township maintenance to prioritize road repair). Circumstances that impact service provider continuity extend beyond physical resiliency (e.g., financial solvency, cybersecurity posture)
- **Establish a back-up plan.** Establish agreements, such as intergovernmental agreements (IGAs) or memoranda of understanding/agreement (MOU/A), with partner entities who can provide back-up services in the case of a sudden discontinuation of service, or secure pre-established back-up service contracts with vendors if procurement policy allows
- **Exercise due diligence.** The pre-planning phase is the best opportunity for public safety agencies to perform due diligence. This process may include (1) analyzing and documenting user needs, (2) understanding the current state of technology, (3) researching available vendors and capabilities (including those in research and development) in the marketplace, (4) examining supply channels, and (5) performing cost and budget analysis. This is the best time to capture the "big picture" for the agency's needs and goals
- **Build relationships and coordinate with key personnel in adjacent or regional jurisdictions.** As a best practice, system planners and administrators might contact system administrators or other key personnel in adjacent, peer, or overlapping jurisdictions, including (but not limited to) personnel such as the following (as applicable):
    - Statewide Interoperability Coordinator (SWIC)[7]
    - state/territorial 9-1-1 administrator[8]
    - system administrators in adjacent or regional jurisdictions or cooperatives
    - CISA Regional Coordinator (RC)[9]
    - state-level or other applicable Communications Units (COMUs) within the National Incident Managements System (NIMS) Incident Command System (ICS)[10]
    - FEMA Regional Emergency Communications Coordinator (RECC)[11]

[7] Information about SWICs can be found on the NCSWIC webpage.
[8] The National Association of State 911 Administrators (NASNA) provides contact information for most state and territorial 911 coordinators.
[9] See the CISA Emergency Communications Coordination Program webpage for general information about CISA RCs and RC contact information; see the NCSWIC membership website for information about CISA emergency communications regions.
[10] CISA provides COMU training and other resources, which are listed on the SAFECOM resources webpage; see the FEMA NIMS webpage for additional information about NIMS, ICS, and COMU.
[11] General information about FEMA RECCs can be found at the FEMA Disaster Emergency Communications Division webpage.

PHASE 02 PROJECT PLANNING

The project planning lifecycle phase is when the agency formalizes the project team, identifies operational and technical requirements for system replacement and upgrade, and develops the project plan. While the previous pre-planning phase necessitates some requirements assessment, the project planning phase involves significant collection of relevant user needs and requirements.

During project planning, agencies might engage in the following recommendations:

- **Identify, assess, and communicate appropriate security and resiliency requirements or plans.** The adoption of emerging technologies and continued use of legacy systems presents a variety of security, reliability, and interoperability concerns. Identifying available resources, increasing awareness, performing risk analysis, considering costs of mitigation, and implementing available guidance[12] can bolster infrastructure protection and communications continuity of operations. For example, to reduce the cybersecurity vulnerabilities presented by third-party partners, public safety organizations can use the the National Institute of Standards and Technology (NIST) Cybersecurity Framework[13] and the following recommendations:
    - Perform planning and due diligence to reduce risks before entering into formal supplier or other third-party relationships, including risks from intential or unintentional disruption of underlying systems (e.g., information technology assets; mobile applications; position, navigation, and timing systems[14])
    - Establish cybersecurity roles and communication routes for third-party partners, ensuring that they understand these roles and responsibilities
    - Identify, prioritize, and assess partners and suppliers of information systems, components, and services using the cyber supply chain risk assessment process
    - Utilize contracts with suppliers and partners to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program
    - Routinely assess suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
    - Conduct response and recovery planning and testing with suppliers and partners
- **Issue requests for information (RFIs) as needed.** [15] Issuing RFIs can help agencies better understand the technical offerings and potential cost ranges of third-party capabilities before agencies release a request for proposal (RFP). This helps agencies identify and outline the full set of technical and functional requirements for a project prior to releasing an RFP, thereby limiting the chances of having to re-release an updated RFP once an agency realizes the full scope of a project's requirements. Reaching out to other agencies who have gone through similar transitions to gain firsthand knowledge of the process for a particular service offering can also prove beneficial

PHASE 03 REQUEST FOR PROPOSALS AND ACQUISITION

The RFP and acquisition lifecycle phase is when the agency selects the appropriate procurement vehicle and, if appropriate, begins the procurement process. This phase does not imply that an RFP

[12] See CISA's Public Safety Communications and Cyber Resiliency Toolkit, an interactive graphic that directs to a collection of government resources for various elements in the public safety ecosystem.
[13] NIST, "Cybersecurity Framework," last accessed April 11, 2024.
[14] GPS for Public Safety Location Services: Use Cases and Best Practices, or use "Understanding Vulnerabilities of Positioning, Navigation, And Timing"
[15] The SAFECOM and NCSWIC *RFP Best Practices for LMR Subscriber Units Procurement Toolkit* is an available resource for understanding the RFI and RFP processes for procuring LMR subscriber units.

must be issued—depending on the system needs, the agency may select another acquisition method, such as a Statement of Requirements (SoR) or Statement of Work (SoW). Additional information regarding procurement and contract documents may be found in Appendix F.

During RFP and acquisition, agencies might engage in the following recommendations:

- **Incorporate resiliency and continuity of operations requirements into acquisition processes.** Developing RFPs and service-level agreements (SLAs) that support resiliency and continuity of operations requirements can help ensure service providers and third parties maintain the continuity necessary to provide uninterrupted service to public safety agencies. Taking the following steps, among others, can help agencies ensure continuity practices beyond agency bounds (See Appendix F for additional information):
    - Require redundancy measures in RFPs and SLAs, including power generator security and safety, established server downtime and outage procedures, and redundant data backups
    - Hold service providers and third parties accountable in legally enforceable ways, ensuring contract terms are met to contract standards
    - Ensure service providers maintain adequate staff or staffing capacity, training and expertise, and resources to address continuity and resiliency needs. Service providers may be open to implementing these measures, if not already in place
    - Confirm that vendors who provide services spanning multiple agencies and jurisdictions maintain infrastructure with the capacity to handle network traffic from all existing and future customers during times of usage spikes
    - Ensure service providers provide reliable 24/7 technical support, if required
- **Follow agency procurement policies and statutory requirements.** When developing RFPs and entering service agreements, officials should adhere to their organization's policies and requirements to avoid acquisition-associated legal or ethical violations, as these complications can later impact service access and the organization's overall ability to perform its regular duties
- **Identify contingency services.** Identifying back-up service providers can help an agency continue operations if a third-party service suddenly discontinues service (e.g., a contracted third-party declaring bankruptcy or a long-term outage). Agencies may want to confirm their budget allows for the sudden cost fluctuations associated with switching or adding service providers prior to establishing these mitigative contracts
- **Confirm that security policies and best practices are followed.** Confirm vendors or service providers are compliant with all relevant federal, state, and local security or operational policies and industry best practices. For example, many states may require in the contract that data is to be maintained or stored only in geographic locations within the United States

The implementation lifecycle phase includes developing an implementation plan, installing new systems or components, training and testing, updating operational procedures, and transitioning to the new or updated capabilities.

During implementation, agencies might engage in the following recommendations:

- **Enhance testing.** Network testing and performance observation are critical for identifying insufficient system component and information sharing attributes. A best practice is for system administrators to incorporate an operational test period—a time for identifying and fixing issues when a new system is operationalized and when the network is fully loaded with the regular traffic that occurs during a large-scale incident

- **Promote and use priority services.** Priority telecommunications services[16] remain key to ensuring communications accessibility during times of network congestion. Enhancing awareness and use of these services among key partners remains key to ensuring emergency communications continuity

The support, maintenance, and sustainment lifecycle phase is typically the longest phase in the system lifecycle. This phase includes maintaining accurate inventories, evaluating performance and maintenance or sustainment needs, executing ongoing maintenance and operations models, and updating the system or its components (such as software updates).

During support, maintenance, and sustainment, agencies might engage in the following recommendations:

- **Maintain proper levels of qualified personnel**. Over the course of a contractual time period, personnel within the agency and within the contracted entity may see changes in personnel and subject matter expertise. Additionally, some third parties may have subject matter expertise within (or outsourced by) their organizations that is not immediately available in the region or relative time zone. To anticipate these changes or constraints, agencies might work with the contracted entity to guarantee that sufficient personnel and expertise levels are either assigned or available according to the agency's contractual requirements. This may require extra coordination and communication between the parties involved, especially if sub-contractors are present. Be aware the internal or external organization may require a transitional period to ensure new or existing personnel are trained
- **Manage cyclical repair, replacement, testing, and training to prevent network or infrastructure issues**. Agencies often depend on multiple external entities to provide services valuable to the operations of their systems, meaning that agencies must carefully manage the maintenance and testing cycles for each of those services. Agencies can follow a maintenance schedule to ensure all system components receive proper, timely care
- **Establish access network redundancy**. To mitigate interruptions in services, agencies might confirm vendors, service providers, and their own organizations maintain redundant access networks, thereby enabling continuity of operations (i.e. those services requiring core network connectivity) in the case of an access network outage
- **Be prepared for catastrophic events.** Be aware that ordinary conditions under which regular agreements or contracted services were predicated may fluctuate as circumstances evolve during force majeure events. These events require redundancy, preparedness and routine testing of inventory and equipment, as well as secondary and tertiary plans for supply of services or provisions (e.g., fuel for power generators, local or remote support personnel, equipment sanitation materials, Telecommunications Service Priority [TSP][17] program use)

The end of lifecycle assessment and replacement lifecycle phase determines when to appropriately replace or upgrade systems or components.

[16] See CISA's priority services webpage.

[17] The CISA-administered TSP program authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment of eligible vital voice and data circuits from commercial service vendors.

During end of lifecycle assessment and replacement, agencies might engage in the following recommendations:

- **Work with service providers to account for technology evolution.** Contracts might commit agencies to certain services for periods of time that outlive evolutions in technology. For example, telecommunications providers often enter indefeasible rights of use (IRUs) that can be termed upward of 20 to 30 years. Even five-year contracts can outlive technological advances, depending on the service. To anticipate such evolutions, agencies can work with service providers to properly manage requirements, capacity, interoperability, and other elements associated with technological evolutions. Some evolutions may require unique acquisition processes, in which case agencies may need to be careful discussing capabilities without first issuing an RFI or RFP. Agencies should consult applicable procurement policy or guidelines in making that determination

The disposition lifecycle phase determines optimal options for decommissioning and dispositioning legacy systems or components. Depending on the circumstances, agencies may choose to dispose of infrastructure, equipment, or other materials; reuse or repurpose old components; sell or gift components to other entities; or return the components to the owning entity (as is the case when equipment or infrastructure is leased).

During the disposition lifecycle phase, agencies might engage in the following recommendations:

- **Ensure non-agency partners properly dispose of materials**. In cases where an agency does not hold responsibility for disposal of non-reusable materials and/or decommissioned equipment used by third parties, agencies might nonetheless confirm that all materials are properly dispositioned in a legal and ethical manner. Be aware that some materials may be non-reusable, and therefore permanently dispositioned, while others may be decommissioned, sold to another party, or recycled. Agencies might be aware of the intent of any non-agency partner to discard or repurpose infrastructure or other components
    - Confirm to the extent possible that any assets containing sensitive data undergo proper erasure. Any components containing data or programming of both sensitive and non-sensitive nature likely require government- or industry-standard data erasure (also referred to as "sanitization").[18] In such instances, improperly dispositioning these assets can pose a cybersecurity threat or expose critical data or personally identifiable information (PII), which could negatively impact resiliency or continuity of operations, as well as subject the agency to legal and public scrutiny. Agencies might work with non-agency parties on conformance to any government or industry data erasure standard and require, where appropriate, delivery of confirmation documentation
    - Confirm to the extent possible that disposal techniques are performed according to current federal, state, and municipal environmental policies. Any discarded or recycled materials should follow Environment Protection Agency (EPA)[19] regulation and other relevant statutes, policies, or guidelines[20]

[18] See CISA guidance on proper disposal of electronic devices.
[19] See the EPA's "Hazardous Waste" webpage.
[20] The EPA has additional guidance on electronics disposal, including references for state electronics disposal laws

Ongoing Activity[21]

Throughout all lifecycle phases, agencies might engage in the following practices to ensure continuity and resiliency:

- **Increase collaboration.** The minimum resiliency and cyber and physical security requirements associated with agency and non-agency infrastructure vary widely. Greater collaboration between stakeholders is encouraged to ensure partners are mutually engaged in continuity of operations planning, governance processes, and the adoption of cybersecurity and infrastructure security best practices
- **Maintain relationships with key personnel in adjacent, peer, or overlapping jurisdictions.** Build and maintain relationships with key personnel in neighboring jurisdictions, with state- or territorial-level communications or interoperability administrators (e.g., SWIC, state-level COMU), and with regional or federal partners (e.g., CISA RC) throughout the system lifecycle, not just when planning the system. These relationship may prove critical during service disruptions such as natural disasters
- **Anticipate and prepare for the unexpected.** Be aware that a variety of unexpected events can suddenly and simultaneously occur, causing operational and other disruptions. These unexpected events could be natural disasters and other force majeure events, industrial accidents, or financial upheavals (such as bankruptcy), and may occur concurrently. Agencies might continually ensure steps are taken throughout the lifecycle to prepare for any forms of disruptions where third parties may be involved or may need to become involved
- **Remain informed about statutory or regulatory changes.** Be aware that federal, state, local, or other legislative, policy, or regulatory changes may impact the communications ecosystem during any lifecycle phase and may vary among jurisdictions. These changes could ultimately impact system requirements, usage, or non-agency partners

Summary

Figure 2 shows the System Lifecycle Planning Guide and the associated recommendations for resiliency and continuity of operations outlined in the sections above.

[21] "Ongoing Activity" is not included in the System Lifecycle Planning Guide.

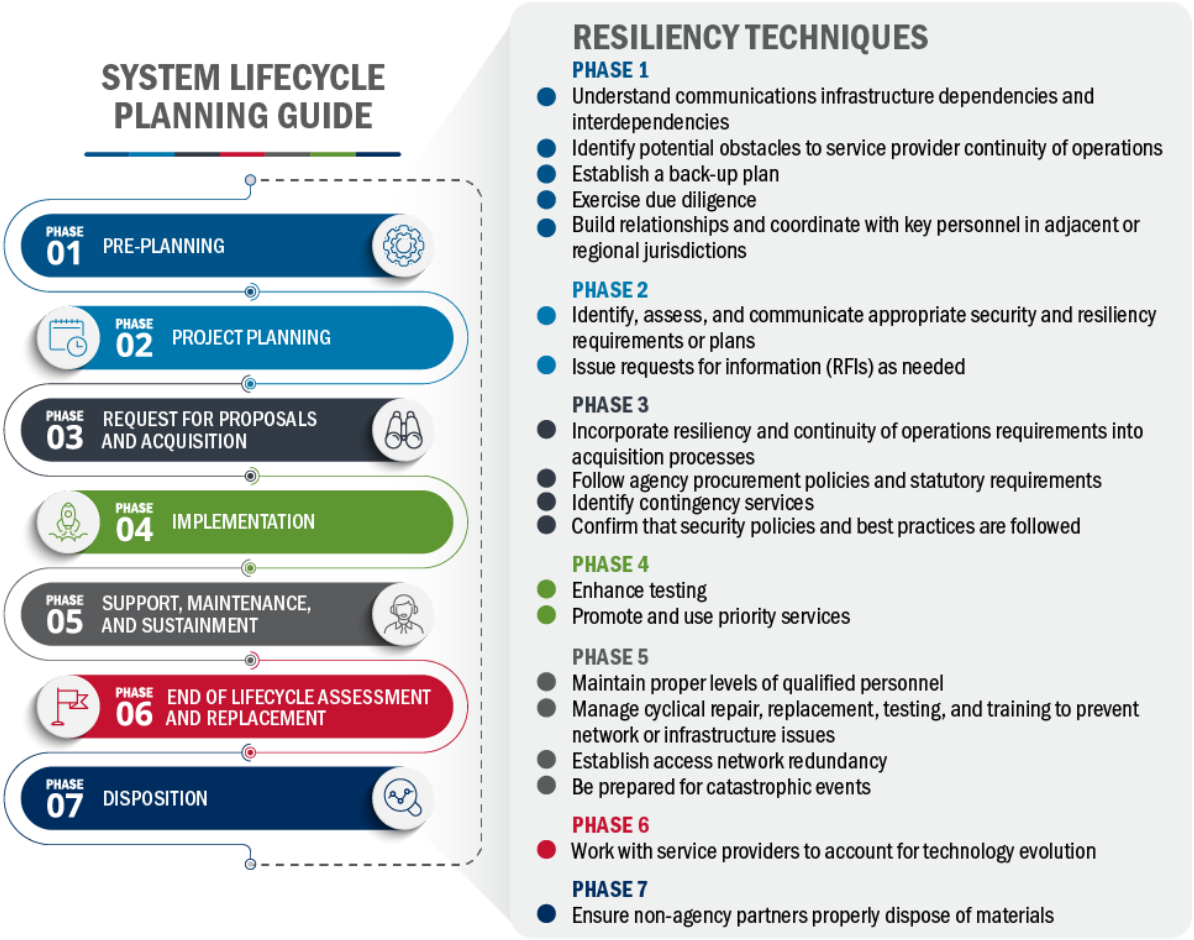


Figure 2. System Lifecycle and Associated Resiliency Techniques

APPENDIX A. COMMUNICATIONS SECTOR COMPONENTS

The Cybersecurity and Infrastructure Security Agency (CISA) identifies 16 critical infrastructure sectors,[22] including the Communications Sector. The Communications Sector is critical because it provides an "enabling function" across all other critical infrastructure sectors.[23] Figure 3 shows the infrastructure components that make up the Communications Sector.[24] These components include the server centers that create the core network, physical transmission lines for delivering and receiving data, and switching stations for routing data across transition lines. Cellular and radio towers, satellites and satellite dishes, and sensors and end-user devices are part of this complex ecosystem and its networks that allow users access to the core network. The use of this infrastructure continues to evolve through network function virtualization, software-defined networking, and network slicing (i.e., the multiplexing of virtualized and independent logical networks on the same physical network infrastructure).

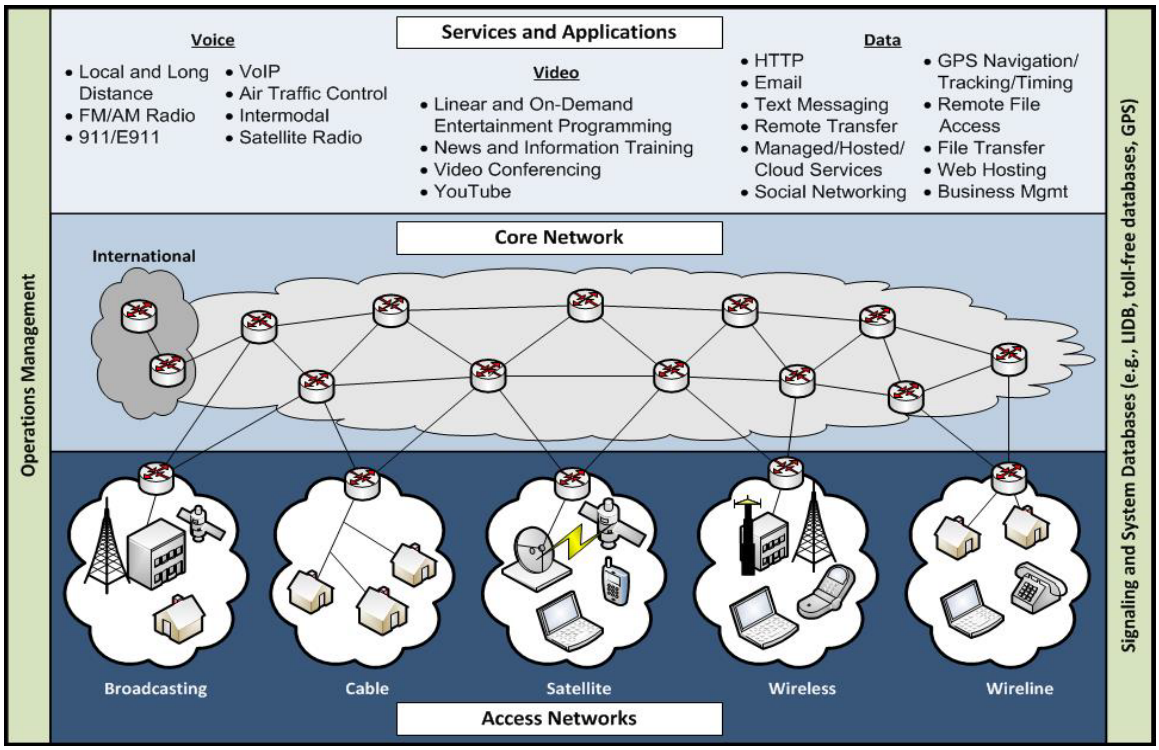


Figure 3. Communications Sector Architecture Model. This model depicts examples of network access methods and services and is not intended to be comprehensive, exact, or authoritative.

What is the Core Network?

Cloud facilities, smaller data centers, and servers all provide computing and data storage services that support the emergency communications ecosystem. These facilities' servers make up the core network, including the network commonly known as the "Internet." Devices transmit and receive information to the core network via access networks. As shown in Figure 3, there is no single core network; multiple service providers operate distinct core networks that interconnect access networks located across the country. Traffic from cellular phone, cable broadband, and wireline users may

[22] See CISA's Critical Infrastructure Sectors for more information.
[23] The White House, "Presidential Policy Directive 21," February 12, 2013.
[24] CISA, "Communications Sector-Specific Plan, An Annex to the NIPP 2013," 2015.

traverse the same core networks. In some cases, the same company that operates access networks may also operate a core network (e.g., Verizon, AT&T).

However, the core network is distinct. Core networks are redundant and resilient because of a high degree of interconnectedness with other core networks, enabling data backups and the ability to reroute traffic around damaged network nodes. Information flows in the form of electrical current, light, or radio waves. It moves between devices and the facilities' servers that make up the core network via data or data packets.[25] These data packets travel across physical transmission lines (e.g., coaxial, fiber optic, twisted pair) or via air/space. As these data packets move through a network, various core nodes (e.g., switches, routers, servers) route the information from one transmission line to another until they reach the access network (e.g., modems, cell towers, radio towers, repeaters, satellites, antennas/satellite dishes) which transmits the information to a device where they are reassembled into a comprehendible form like sound, imagery, video, or text.

What are Access Networks?

Access networks connect end-user devices to the core network and are made available primarily through commercial service provider infrastructure. The following are six types of access networks.

1. **Broadcast networks** use radio waves to transmit analog and digital audio and video across radio frequency bands (e.g., amplitude modulation [AM] radio, frequency modulation [FM] radio, television)
2. **Cable networks** use electrical current and light via a hybrid fiber and coaxial (HFC) cable to transmit data. Analog and digital video, analog television (TV), and high-speed broadband services (i.e., high-speed Internet) are all provided across cable networks[26]
3. **Satellite networks** use radio waves to transport a wide range of information. This information is transmitted by antennas on the surface of the earth to an orbiting satellite and then relayed to another antenna on the earth's surface. These receiving antennas may be a component of a device (e.g., a satellite phone) or connected to infrastructure (e.g., a terrestrial antenna), which then conveys the data across other networks to its endpoint(s)
4. **Wireless networks** transmit information using radio waves through cellular phones, wireless hot spots (Wi-Fi), high-frequency radios, personal communication services, and unlicensed wireless platforms to single network access points[27]
5. **Wireline networks** consist of circuit- and packet-switched networks of copper, fiber optical, and coaxial cables to transport media. Wireline networks are made up of private enterprise data and telephony networks. These networks constitute the core backbone of the Internet and support the public switched telephone network by carrying the information from access points and networks through resilient and redundant pathways[28]
6. **Mesh networks** leverage the Internet of Things (IoT) to connect devices and transmit data. In mesh networks, devices connect to the network through other devices within their proximity, each acting as a node in the greater network. Data flows from device to device and eventually connects to an access point[29]

In most cases, an incident requiring public safety response will not impact the core network but may degrade the access networks. As demonstrated in Figure 3, access networks have fewer redundant

[25] A data packet is a portion of an entire piece of information (e.g., a video clip, email) that is broken down into smaller units (i.e., a serious of 1s and 0s) so that it may travel across a network. Data packets may travel along a different route in their journey to a device. Once a device receives these data packets, it reassembles and converts them into digestible information. Each data packet contains the Internet Protocol (IP) addresses of the device sending the information as well as the device meant to receive the information, thereby ensuring the correct device(s) receives the data, and that this device(s) knows where the data originated.
[26] CISA, "Communications Sector-Specific Plan, An Annex to the NIPP 2013," 2015.
[27] Ibid.
[28] Ibid.
[29] The President's National Security Telecommunications Advisory Committee (NSTAC), "NSTAC Report to the President on Emerging Technologies Strategic Vison," July 14, 2017.

connections as they get closer to the user. Specifically, the access network in a local area may rely on a key facility for connectivity to a core network; damage to the key facility could disrupt network access. Also, since access networks are designed to support "steady-state" operations, they may become congested during emergencies. Alternatively, the core network has more redundant connections and greater capacity. If a key hub (e.g., a server facility) or transmission line fails, the core typically continues to function.

Some emergency or operational scenarios may necessitate temporary increased reliability, connectivity, and/or capacity on an access network, such as reliance on a privately-owned commercial internet protocol (IP) network (e.g. home or commercial Wi-Fi network). In these cases, the end-user devices continue to connect to the core network via those access networks.

What are Sensors and Devices?

Communications sensors and devices leverage access and core networks to transmit and receive data. In this context, the following example devices and networks may serve as unidirectional transmitters or receivers:

- Emergency beacons that only transmit location data
- Smart city sensors that only transmit gunshot, hazmat, or fire/smoke data
- Handheld global positioning systems (GPS) that only receive location data from satellites
- TVs that only receive video data

An increasing number of devices and apparatus have the capability to communicate bidirectionally, including:

- Phones (e.g., terrestrial, satellite, cellular)
- Computers
- Gaming consoles
- Two-way radios
- Smart vehicles
- Deployable incident support vehicles and command centers
- Unmanned aerial systems (UAS)

Depending on the configuration of these devices, they may transmit and receive a range of data across commercial network infrastructure. With access to the Internet, they may use various capabilities (see "Services and Applications" row in Figure 3) for the transmission and receipt of emergency communications. Technology—including Internet-connected devices, software, and applications—facilitates information sharing across networks. This interconnected and interdependent system of infrastructure, networks, and devices enables emergency information sharing and is key to ensuring successful public safety communications, operations, and response.

Variation in Communications Infrastructure

Communications infrastructure may vary depending on a number of factors, including geographic, demographic, budgetary, mission, functional, and historical (legacy) requirements. For example, the communications infrastructure of a remote, rural region may have some distinctive or different characteristics from that of a dense metropolitan area; regions stretching across mountainous terrain or dense forest may likewise require different approaches to the communications ecosystem. While the general Communications Sector components still apply, public safety communications administrators might consider the potential for customization in the communications infrastructure which may impact dependencies on non-agency entities for core or access network components.

APPENDIX B. 911 EXAMPLE DEPENDENCIES

Servicing emergency calls from the public is one of the most common and critical functions of public safety communications. Emergency Communications Centers (ECCs)/ public safety answering points (PSAPs)[31] might rely on non-agency entities to transmit, document, store, or protect voice communications, imagery, video, text messages, location, or other data. Third-party infrastructure (e.g., "as-a-service solutions") and supplemental data providers (e.g., supplemental location and/or health data) are also becoming more common.

911 Real-World Network Outage

"On March 8, 2017, and again on May 1, 2017, AT&T's wireless phone customers across the country experienced 911 service outages on the company's Voice over Long-Term Evolution (VoLTE) network. Planned network changes implemented by AT&T on those days inadvertently interfered with the company's routing of 911 calls. The March outage lasted approximately five hours, resulting in the failure of 911 calls from some 12,600 unique users. The May outage lasted approximately 47 minutes, resulting in 2,600 failed 911 calls. The [Federal Communications Commission's (FCC)] investigation also found that, during the March outage, the company failed to quickly, clearly, and fully notify all affected 911 call centers."[30]

When a caller dials 911 via phone, their voice data transmits from their device either through a wireline connection or to a wireless tower and into a base station. These base stations are often owned by commercial wireless service providers that use the tower to provide broadband connectivity to their subscribers; certain providers pay to use base stations that they do not own to provide service to their subscribers. This signal is then sent to a mobile switching center (MSC) that is operated by the caller's service provider. This MSC reads the transmission's information and routes the data to the appropriate 911 tandem/selective router, which then forwards the call and its associated information[32] to the appropriate ECC/PSAP. The ECC/PSAP then dispatches services to the caller's location. In short, a 911 call originating from a cell phone must transmit across the commercial service provider's infrastructure before it reaches agency-owned and operated network components (e.g., customer premises equipment [CPE]) supporting the ECC/PSAP.

[30] FCC, "FCC Settles Investigation Into Two AT&T Mobility Nationwide 911 Outages in 2017," June 28, 2018.
[31] The term ECC/PSAP encompasses PSAPs, public safety communication centers (PSCCs), 911 communication centers, Emergency Operations Centers (EOCs), Security Operations Centers (SOCs), or any other call center operated for the purpose of receiving and dispatching calls for services. These centers may also have other systems co-located at their facility and provided through interconnected infrastructure, including alerts, warnings and notification (AWN) systems, 311 systems, or other non-emergency numbers and public safety communications systems.
[32] Depending on available capabilities, 911 calls may contain the caller's voice transmission, information about their approximate or exact location (based on the transmitting cell tower or GPS within the device itself), and a call-back number.

APPENDIX C. LAND MOBILE RADIO EXAMPLE DEPENDENCIES

Land mobile radio (LMR) systems are the primary means for public safety agencies to achieve critical voice communications. These systems are vital for ensuring safe and effective operations and may be owned, operated, and maintained by federal, state, local, tribal, and territorial governments. Agencies might depend on non-agency entities for components of the LMR system infrastructure (e.g., repeaters), as well as other system requirements such as operation and maintenance; network monitoring, restoration, or troubleshooting; and generator fueling.

LMR Real-World Network Outage

"FirstNet provided the city of Whiteville, N.C., with critical voice and data communications throughout Hurricane Florence and subsequent flooding in the area, passing a 'big test' regarding the resiliency and flexibility associated with the Nationwide Public Safety Broadband Network (NPSBN)…Hal Lowder, director of the emergency operations center in Whiteville, NC, said that FirstNet played a vital role in the city's recovery efforts, particularly after the failure of its LMR system—a county-owned 400 MHz trunked system that uses a proprietary technology. Whiteville public safety, city officials and some mutual-aid personnel were able to maintain communications by using…enhanced push-to-talk service (EPTT) over the FirstNet system without interruption. 'There were times there when EPTT was our primary means of communications,' Lowder said."[33]

To communicate via LMR systems, an individual uses a mobile or portable radio device (i.e., a subscriber unit) to broadcast a signal to a repeater and ultimately to base stations and other end users operating on the same channel or talk group. In larger networks, these repeaters and base stations can be connected over IP networks that allow LMR systems to increase capacity and reliability over geographically diverse areas.[34] In the instances where an LMR system integrates with an Internet protocol (IP) network, public safety agencies must gain access to the Internet through an Internet service provider (ISP).

Portable two-way radios, repeaters, base stations, and other LMR equipment must be acquired from private sector manufacturers, making users dependent on these supply chains. In many cases, agencies may affix antenna systems and place repeaters and other system components on or within privately owned structures from which they lease space.

Due to the criticality of their mission, public safety agencies and their respective governments must design and implement robust, resilient, and redundant LMR systems. These networks may be designed and implemented to higher resiliency standards than those of commercial wireless carriers. For example, during 2018 Hurricane Michael, cellular capabilities were severely compromised, forcing first responders to solely use LMR systems for their communications.[35] However, in extreme cases, LMR systems are also susceptible to outages caused by natural and manmade disasters, human error, and other technical issues.[36,37] Some agencies have opted to use public safety-specific broadband networks to provide additional resiliency measures.[38]

[33] Donny Jackson, "North Carolina City Relies on FirstNet Voice, Data Communications During Hurricane Florence," September 26, 2018, last accessed September 3, 2020.
[34] GAO-07-301, "First Responders: Much Work Remains to Improve Communications Interoperability," April 2, 2017.
[35] Peter Schorsch, "Hurricane Michael Emphasizes the Need for Public Safety Radio Communications," *Florida Politics*, November 26, 2018, last accessed September 3, 2020.
[36] Damian Trujillo, "Radio Silence: Sunnyvale Police Officers Were Unable to Communicate with Dispatch," *NBC Bay Area*, June 11, 2018, last accessed September 3, 2020.
[37] Brittany Wallman, "Radio Outages Plague 911 Responders," *Sun Sentinel*, September 24, 2014, last accessed September 3, 2020.
[38] Donny Jackson, "Florida City Turns to AT&T, FirstNet for Connectivity During Aftermath of Hurricane Michael," *Urgent Communications*, October 26, 2018, last accessed September 3, 2020.

APPENDIX D. BROADBAND EXAMPLE DEPENDENCIES

Given communications rely heavily on commercially provided broadband access, responders may be unable to fully use Internet-connected devices and mobile applications when this infrastructure is interrupted. For example, 95 percent of cell towers in Puerto Rico were non-functional following Hurricane Maria in 2017, which significantly hampered response efforts and caused officials to use paper forms and offline devices to process assistance requests.[40]

Broadband Real-World Network Outage

"Following Hurricanes Irma and Maria in 2017, [the Federal Emergency Management Agency (FEMA)] deployed Disaster Survivor Assistance teams across Puerto Rico. Since these teams typically use tablets with cellular and wireless broadband access, limited service hindered their efforts to register survivors for disaster assistance and conduct case inquiries and updates. In the absence of mobile communications, teams used paper registration forms and offline laptops and tablets. These new, non-standard processes caused inaccuracies and omissions, delaying the provision of aid. Limited commercial communications and user unfamiliarity with contingency communications options also impacted command and control activities, including resource requests. Staff used handwritten resource requests and subsequently had to review, prioritize, sign, scan, and manually enter more than 2,000 requests into FEMA's crisis management system, further contributing to delays."[39]

This event demonstrated that even commercial broadband communication networks designed for priority public safety use[41] cannot ensure constant connectivity during times of network outages. Since owners of commercial communications infrastructure are generally responsible for the repair of their property, network access may still be slow to return in the face of a disaster, even when government entities offer support (e.g., loans, contract acquisition). To lessen the impacts of these outages, emergency management agencies might ensure alternate communications platforms (e.g., satellite-enabled devices, mobile repeaters, mesh networking) are available to enable responder-to-responder communications, core network connectivity, and provisional public connectivity. Additionally, protection of critical commercial communications nodes, including extensive and redundant perpetual backup power, multiple paths to backhaul network traffic, and site hardening, can help mitigate these risks.[42]

[39] FEMA, "2017 Hurricane Season FEMA After-Action Report," July 12, 2018.
[40] Ibid
[41] Examples of these networks include the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and TSP programs.
[42] Jill Gallagher, "The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress," *Congressional Research Service*, April 27, 2018.

APPENDIX E. CLOUD-BASED SERVICE OFFERINGS EXAMPLE DEPENDENCIES

Agencies responsible for public safety communications are increasingly using or migrating to service offerings within the cloud computing architecture to support public safety communications systems.

Cloud computing architecture consists of hardware resources including computers (central processing unit [CPU] and memory), networks (routers, firewalls, switches, network links, and interfaces), and storage components (hard disks). Cloud facilities also include resources like heating, ventilation, and air conditioning (HVAC), power, and other physical infrastructure elements.[44] Cloud computing is available in many different service and deployment models.[45]

Cloud Real-World Network Outage

"A disruption in Google's network in parts of the United States caused slow performance and elevated error rates on several Google services, including Google Cloud Platform….Because the disruption reduced regional network capacity, the worldwide user impact varied widely....For users who rely on services homed in the affected regions, the impact was substantial, particularly for services…which use large amounts of network bandwidth to operate….The root cause of [the] disruption was a configuration change that was intended for a small number of servers in a single region. The configuration was incorrectly applied to a larger number of servers across several neighboring regions, and it caused those regions to stop using more than half of their available network capacity. The network traffic to/from those regions then tried to fit into the remaining network capacity, but it did not…. Engineering teams quickly identified the cause of the network congestion, but the same network congestion which was creating service degradation also slowed the engineering teams' ability to restore the correct configurations, prolonging the outage."[43]

Leveraging cloud infrastructure can prove beneficial for a range of reasons including enabling "anywhere" access and resource-efficient data storage, as well as the ability for on-demand information sharing, monitoring usage across the network, and rapid data usage scalability. As a result, a variety of emergency communications systems are available or supported by cloud services including artificial intelligence (AI) and Internet of things (IoT) sensors; alert, warning, and notification (AWN) systems; audio and video recording; computer aided dispatch (CAD); crisis management systems (CMS); email; geographic information systems (GIS); land mobile radio (LMR) systems; records management systems (RMS); and website hosting.

Still, cloud-based delivery often means that network administrators have little knowledge or control over where data is flowing or stored. Proper engineering is therefore necessary to ensure data security and backups, redundancy for continuity of operations in the case of an outage, and priority data delivery during times of congestion for public safety communications. Additionally, although cloud services are generally more resilient due to their high level of redundancy, misconfigurations or programing errors, as well as impacts to cloud facilities and upstream critical infrastructure sectors, can still lead to outages.[46,47] Access network outages can also disrupt connections to the core network, making cloud computing resources inaccessible. When a non-cloud-based service provider experiences a network disruption, neighboring or backup facilities may remain operational, but if a cloud service provider experiences an outage, many subscriber facilities may be impacted.

[43] Google Cloud, "An update on Sunday's Service disruption," June 3, 2019, last accessed September 3, 2020.
[44] Annie Sokol and Michael Hogan, "National Institute of Standards and Technology (NIST) Cloud Computing Standards Roadmap," NIST, July 2013.
[45] To better understand service and deployment models, refer to NIST, "The NIST Definition of Cloud Computing," September 2011.
[46] S. Srinivasan, "Building Trust in Cloud Computing: Challenges in the Midst of Outages," *Proceedings of Informing Science & IT Education Conference*, 2014 (pp. 305-312).
[47] Valerie Lucus-McEwen, "How Cloud Computing Can Benefit Disaster Response," *Emergency Management*, May 7, 2012.

APPENDIX F. PROCUREMENT AND CONTRACTUAL DOCUMENTATION

Request for Proposal, Contract, and Service-level Agreement

Three significant documents in addressing dependencies on non-agency infrastructure and services include the Request for Proposal (RFP), the contract itself, and the service-level agreement (SLA), which is typically included as an appendix in the contract. These three documents provide a strong foundation of expectations between the agency and the contracted infrastructure or service provider(s).

Table 2, Table 3, and Table 4 include descriptions of the RFP, contract, and SLA, respectively; a summary of the purpose or role that these documents play in preparing agencies for dependencies on commercial vendors and suppliers; and example applications demonstrating how agencies might include dependencies-specific content. The example applications are intended as examples *only* and are not intended to provide RFP, contract, or SLA language or make policy, legal, or requirement recommendations. Agencies are encouraged to consult procurement policy or officers, along with all other applicable laws, statutes, or guidance concerning procurement and contractual agreements.

Table 2. Requests for Proposal

Request for Proposal (RFP)	
Description	The RFP is a call for commercial vendors or suppliers to submit proposals to the agency to fulfill the agency's RFP-identified technical or administrative requirements. The RFP includes details regarding the technical requirements and specifications, terms and conditions, and specifications for compliance with administrative regulations, policies, or guidelines. Additionally, the RFP will provide specifics about response formatting, deadlines, and appropriate communications during the response period. The RFP (and successful responses) in many instances may be included as an element (e.g., appendix) in the contract.
Purpose/ Role	The RFP can be used to set expectations regarding dependencies prior to acquisition and contract negotiation. By outlining requirements in the RFP, vendors are able to see up front what the agency expects as part of its future agreement with a non-agency entity. Also, the agency may describe the existing infrastructure or configuration to make vendors or suppliers generally aware of current system operations or requirements. The RFP may also detail requirements for testing and training when transitioning to new capabilities.
Example Applications	Example 1 In the RFP, an agency can state requirements for high levels of redundancy for infrastructure, fiber networks, power generation, or other relevant capabilities as required by the agency. Example 2 In the RFP, an agency might provide as a requirement resource availability in the event of a disruptive event, such as remote or in-person support that is available 24/7 during a force majeure event or other emergency.

Table 3. Contracts

Contract	
Description	The contract is the legally binding agreement for exchange of goods or services between the agency and non-agency vendor or supplier.
Purpose/ Role	The contract spells out specific terms and conditions regarding the services that the contracted entity is providing, which might include metrics or performance measures. These terms and conditions are legally binding; therefore, the agency should expect the fulfillment of the terms under the stated conditions. The contract may stipulate that failure to perform services or breach of contract may result in appropriate forms of redress.
Example Applications	Example 1 In the contract, language might address specific redundancy measures as a requirement under the contract, such as stating that data (both primary and backup) stored, maintained, or transmitted in the cloud must be hosted on servers geographically located within the continental United States. Example 2 Many contracts include clauses addressing force majeure events (events such as acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, and embargoes or blockade). While these clauses normally provide flexibility in performance or execution of the contract in the wake of a force majeure event or provide an avenue to release liability for damages caused by such events, agencies might also include language that requires certain performances even under force majeure circumstances.

Table 4. Service-level Agreements

Service-level Agreement (SLA)	
Description	The SLA is the agreement used to define the relationship between the agency and the contracted provider and provide greater detail about the services rendered, uptime, and performance, including any performance measures, metrics, quality, or other expectations. The service-level implementation activities are clearly defined. The SLA is typically included as an appendix to the contract and may be enforced in a similar legal manner as the contract terms (consult a legal expert before determining legal enforcement standard). However, the SLA can be modified throughout the life of the contract, depending on need.
Purpose/ Role	Many of the performance activities during events that threaten continuity of operations will be included in the SLA. The contract may bind the third-party entity to provide a specific service; in accordance, the SLA may include specific language regarding the expected performance of the third-party entity during an event disrupting the contracted service to ensure required service levels are maintained. The SLA defines with granularity the performances to which both the agency and the contracted party agree. Additionally, support levels and availability—such as monitoring, field service, or helpdesk support—may be described.

Service-level Agreement (SLA)	
Example Applications	Example 1 The SLA may have operational guidelines around redundancy measures, such as simultaneous operation of a remote "mirror system" that is identical to the primary system and/or has data backup capabilities. Example 2 The SLA may outline details regarding performance during a force majeure event, provide guidelines regarding suspension of performance, and/or specify exclusions and non-suspended obligations. Example 3 The SLA might state that the agency maintains the privilege to view the third-party entity's Continuity of Operations (COOP) Plan at any time upon request.

Other Agreements and Documentation

In addition to the RFP, contract, and SLA, other procurement, legal, contractual, or operational documents are commonly used by agencies. These documents may also play a role—whether at the agreement or implementation level—in helping agencies properly address dependencies on non-agency infrastructure and services. Document descriptions are presented in Table 5.

Table 5. Additional Procurement, Legal, and Operational-level Documents and Agreements

Document	Description
Continuity of Operations (COOP) Plan	The COOP Plan defines the procedures and plans for continuity of essential services in the event of service disruption. The COOP Plan is typically defined by the third-party provider, and while it may not be part of any agreement between the agency and the third-party provider, the agency may still require access to the provider's COOP Plan upon request.
Indefeasible Right of Use (IRU) Agreement	The IRU is a contractual lease agreement between owners of a telecommunications system and the subscribing customers. In this type of agreement, the customer purchases a defined capacity amount of the system over a specified timeframe. These agreements can often last longer than ten years; some may operate up to 30 years.
Intergovernmental Agreement (IGA)	The IGA, also referred to as Interagency Agreement or Intergovernmental/Interlocal Cooperative (IGC/ILC), is an agreement between two or more government entities (e.g., agencies or departments) that defines the cooperative use of infrastructure or services among those party to the agreement.
Memorandum of Understanding (MOU)	The MOU or Memorandum of Agreement (MOA) is a form of agreement between government entities (often in different spheres of jurisdiction, such as federal and state jurisdictions). Common forms of MOUs are between federal and state or tribal entities, but can also extend to agreements between other government entities.
Request for Information (RFI)	The RFI is used to solicit information from the market prior to the issuance of a Request for Proposal (RFP). This document allows agencies to understand more about capabilities in the market and associated technical requirements, and assists agencies in determining if an RFP will be pursued.
Request for Quotation (RFQ)	The RFQ may be issued prior to, or in some cases in place of, the RFP. This document requests a quote and cost model for services to be provided, potentially including details such as payment terms. Certain industries may use alternative nomenclature, such as Calls for Bids (CfB) or Invitation for Bid (IfB), to describe the RFQ document.

Document	Description
Statement of Requirements (SoR)	The SoR outlines technical and operational requirements and communicates associated user expectations and technical standards. In some contexts (e.g., software requirements), this document may be referred to as a User Requirements Document (URD) or User Requirements Specification (URS).
Statement of Work (SoW)	The SoW is a project management document that clearly defines project objectives, scope of work, tasks and deliverables, expected outcomes, and other implementation activities related to a specific project under the contract.