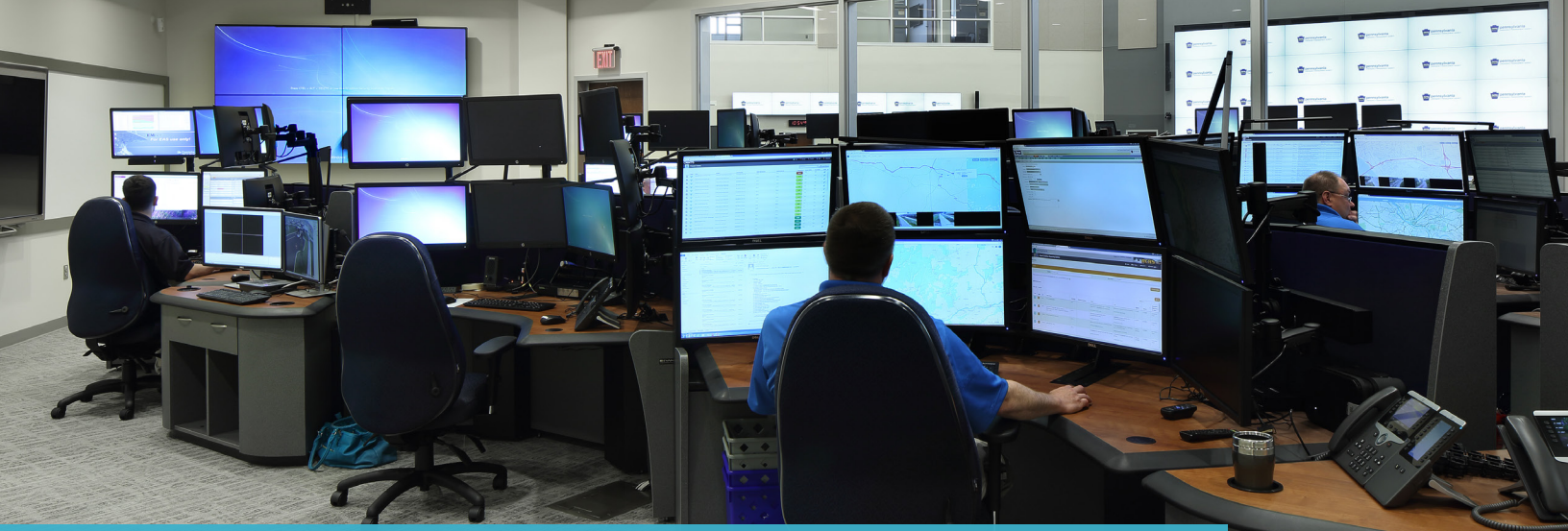

**Whitepaper:** Remote Operations

## BACKGROUND

The COVID-19 pandemic created a public-health crisis that is affecting organizations across the country. In this unprecedented time, it is important for public safety agency and emergency communications center officials to understand the options that will enable them to maintain operations in the event of a full or partial facility evacuation.

In this whitepaper, Mission Critical Partners identifies scenarios and options that agencies can leverage if remote operations become necessary.

# Maintaining Public Safety Answering Point and Emergency Communications Center Operations Remotely During a Public-Health Crisis

## Introduction

As the COVID-19 pandemic continues to evolve, public safety, law enforcement, and other mission-critical response agencies should prepare for the possibility that they may need to mobilize call takers, dispatchers, and other staff members for remote work to protect their health and safety. What is remote work? According to Remote Year, a program that enables participants to temporarily work in their current jobs in cities around the world, remote work is a style that allows professionals to work outside of a traditional office environment and is based on the concept that work does not need to be executed in a certain place to be executed successfully.[1]

There is no one-size-fits-all solution for developing a remote work plan for your agency. Organizations already may understand remote work options as part of an existing continuity-of-operations plan (COOP) or standalone bug-out plan, but this is not the case for all agencies. At a minimum, agency leaders should know their relocation or remote work options and the personnel, policy, operational and technical challenges each presents.

## The Impact of a Public-Health Crisis on Mission-Critical Operations

A place to start is with the checklist developed by the National Emergency Number Association (NENA)[2] for mission-critical organizations to help them navigate the policy changes necessary to protect staff members from the spread of viral illnesses. While this is an evergreen document that will be updated as the coronavirus crisis evolves, it addresses several areas where agencies can adjust operational policies immediately—including social distancing, mental and physical wellbeing, public information and workspace sanitation—to keep employees safe.

In addition, agencies need to be prepared to consider how these challenges will impact short-term and long-term operations, as follows:

- **Environment**
  - Is there a secondary space within the facility that has not been exposed and can be leveraged during this time?
  - If a secondary space is not available within the facility, is there an outside space that can be used? If so, where is it located?
  - Where will staff members rehabilitate and/or sleep if they are required to remain onsite?

MissionCriticalPartners

- **Operations**
  - What is the hierarchy of services that will be provided based on the location and technology available? Which tools and operational or technical platforms can or cannot be moved or transferred to an alternate site?
  - What needs to be done at an alternate site, or sites, to support and sustain necessary mission-critical functions?
  - How will oversight, including supervision, be provided during remote operations?
  - What are the criteria for staff members to be authorized to work from home?
- **Support**
  - Who are the technical and system administration personnel or vendors that can support operations in multiple remote locations?
  - What equipment is available to accommodate staff members to work in remote locations, including from home?

These questions may be very easily answered with minor interruptions to service for some centers. Others will face considerable challenges that include major interruptions to service, such as transitioning to manual computer-aided dispatch (CAD) and using portable radios for dispatch. While working through the major challenges that will need to be addressed, agencies still can determine the best path for moving forward that will meet their organizational needs, and those of the communities they serve, while maintaining the health and safety of staff members. There are several options available to agencies to maintain operations even in a remote environment, such as a secure, reliable home setup:

| SCENARIO | PROS | CONS |
|---|---|---|
| **Shelter in Place.** Agency has elected to remain at its primary ECC facility | • Agency remains fully functional with access to all equipment and technology | • May lose workspace by following CDC social-distancing guidelines<br>• May need to reduce staff due to loss of workspace<br>• Potential for illness exposure and spread |
| **Multiple-Site Operations.** Agency has elected to set up and deploy some staff members to a secondary space (e.g., another space within the primary facility, a mobile command vehicle, or a remote space like a school or home), in addition to working from the primary ECC facility | • Staff members remaining in the primary ECC continue to be fully functional with access to all equipment and technology<br>• Separation of staff members supports social-distancing guidelines and enables regular cleaning and disinfecting of spaces without interruption to operations<br>• Network drops can be pre-run and left in place for future support | Secondary or backup sites may not be fully equipped or networked:<br>• Hardwired equipment may lose some functionality if it is moved to a secondary space— e.g., emergency management agency (EMA) phones, National Crime Information Center (NCIC)<br>• May lose the ability to tone fire/rescue units or monitor secondary channels<br>• May lose some functionality, such as text-to-911 |
| **Full Evacuation**. ECC staff is evacuated from the primary facility completely to a backup facility or for remote work, either temporarily or long-term | • Allows primary ECC to be cleaned and disinfected<br>• Enables staff to work from different locations, limiting illness spread if an employee is exposed | • Access to equipment and technology may be limited<br>• Backup center may become contaminated<br>• May lose some or all functionality in hardwired equipment |

## The Remote Work Decision

The decision to move operations to a remote environment is not one that is made lightly. There are many technical and operational challenges to remote operations and the approach to addressing those challenges may look different for each agency. When making the decision to move to remote operations, agency leaders will need to consider three primary factors:

1. **Options**

   a. **Activating a Traditional Backup Center.** This is the typical method for using backup concepts. ECC staff is evacuated and deployed to work in a backup ECC, and 911 and 10-digit, non-emergency numbers are forwarded to the backup center. The agency may lose access

to primary equipment and technology, as well as some functionality—including access to radio channels and text-to-911—in this process. Additionally, combining staff members from the primary and backup centers could increase the risk of exposure for everyone.

b. **Use of a Secondary Backup Location.** This entails leveraging a location that typically is not used for an ECC but offers the ability to handle the equipment and enables telecommunicators to operate efficiently and with most of the capabilities that are needed. This space must include the resources to answer, process, and dispatch calls for service and typically includes mobile command centers, rooms within the primary facility, or other government or municipal buildings with strong connectivity. Like a traditional backup center, 911 and 10-digit, non-emergency numbers will need to be forwarded and agencies will lose access to primary equipment and technology, as well as functionalities such as access to radio channels and text-to-911.

c. **Leveraging a Non-Traditional Space.** This entails using a location that does not function as an ECC, but provides the resources to do so, including the ability to house and/or rehabilitate telecommunicators, such as a school or hotel. With this option, 911 and 10-digit, non-emergency numbers will need to be answered using an offsite solution like CommandPost or 911 Go Bags.

d. **Deploying Staff to Work from Home.** With this option, staff members are equipped and deployed to work from home. While this option helps to limit illness exposure and spread by dispersing staff members outside the primary ECC facility, it poses additional challenges, such as equipping staff, providing access to technology, loss of some functionality—including radio—and increased cybersecurity risks.

2. **Equipping Staff.** Regardless of the selected option for remote work, backup centers and staff members will need to be properly equipped to execute their core functions. This includes ensuring that staff members have access to computer equipment, call-handling equipment (CHE)—including hardware and software— voice over Internet Protocol (VoIP) or private branch exchange (PBX) phones, and a reliable, secure internet connection. It also includes providing staff members with the means to access mission-critical data and systems, including but not limited to:

   - 911 CHE
   - CAD
   - Radio
   - Telecommunications device for the deaf (TDD)/teletypewriter (TTY)
   - Alarm calls
   - NCIC

3. **IT Considerations.** Remote work for public safety agencies, particularly if staff members are being deployed to work from home, poses several information technology (IT) challenges. While a reliable, secure internet connection is required for telecommunicators to work remotely, it is also imperative to establish a secure virtual private network (VPN) via which staff members can access critical systems and technology. Policies for personal use of agency equipment while working from home also should be established to protect networks and communications.

**Developing Remote Work Plans.** Remote work plans should be established as part of continuity-of-operations plans (COOPs). However, as instances like the coronavirus pandemic have demonstrated, it is difficult to imagine every possible scenario during the planning process. To deploy staff members for remote work in an unplanned scenario, agencies will need to quickly decide how to overcome some key challenges, as follows:

1. **Call Handling.** CHE configurations fall into three primary categories: premises-based, host/remote, and cloud-based, i.e., call handling as a service (CHaaS). Premises-based and host/remote are the most common design approaches to call handling; however, cloud-based solutions increasingly are being viewed as a viable option. Each configuration poses its own set of operational challenges as it pertains to remote work. While solutions providers strive to deliver standardized platforms and service offerings, there are unique components to every implementation. Therefore, upfront planning is paramount to successfully maintaining operations. Additionally, because of the unique nature of the applications, the technical approaches outlined here may be layered with operational elements to create a more customized solution to an agency's remote call-handling needs.

   There are other factors to consider related to remote call-taking activities, including the type of network that supports call delivery to the ECC (voice and data). Legacy networks can present a greater challenge to a quick shift in operations if not appropriately planned, whereas Next Generation 911 (NG911)-supported solutions may offer a greater level of flexibility in routing choices.

Key considerations for any CHE operational shift include:

- CHE application and hardware (including licensing)
- Provisioning of user data/profiles
- Network connectivity and security
- Access to data and systems (CAD/radio/management information system (MIS)/recording/automatic location identification (ALI)/NCIC/Criminal Justice Information System (CJIS)
- VoIP/PBX phones
- Alternate-routing capabilities
- Reducing user screen footprint

| **OPTION 1:** *Alternate Routing* | **OPTION 2:** *Mobile and Backup Centers* | **OPTION 3:** *Remote Call Handling* |
|---|---|---|
| Legacy ECCs may have an "abandon button" or a pre-coordinated plan with the selective-routing provider to reroute traffic to a neighboring agency or backup center<br><br>NG911-compliant ECCs likely have policy-based routing established to support alternate routing during disasters. This may have a web-based abandon feature or require provider coordination<br><br>This option always should be preplanned when outside agencies are supporting alternate-routing capabilities. Alternate-routing measures are intended to be short-term, stopgap measures only | Some agencies may have the ability to move operations to mobile command centers or backup ECCs with equipment pre-staged and configured. This option often will require similar coordination and planning to Option 1, whereby legacy and/or NG911 providers need to "swing" traffic to other facilities, offering a longer-duration support model and the ability to support fully functional ECC operations | Instances where agencies must completely evacuate their primary facility and do not have access to a backup or secondary facility may require more creativity to continue operations beyond an immediate alternate-routing solution as outlined in Option 1<br><br>The ability to shift to fully remote call-taking operations will vary in difficulty depending on an agency's existing CHE. In terms of operational flexibility, the best option for remote call handling is a cloud-based, or CHaaS system. A premises-based system is the most difficult to transition from an agency environment to a remote work setup |

While pre-planning and coordination are key to successfully transitioning call-handling operations from an ECC to a remote environment, there are short-term solutions available in the event of a call center evacuation. These scenarios are not without their own challenges, including available IT support and budget constraints, however, and it is important to understand the limitations of existing CHE in the event remote operations become necessary.

2. **CAD.** Accessing data from CAD or other applications in use at ECCs typically is established via a web-based application or an installed thick client on a Windows-based workstation. The CAD application supports and usually requires multiple screens to display all relevant information needed to appropriately dispatch emergency responders. To accommodate remote dispatching access to these applications, the following requirements need to be met at the remote location:

    1. Network connectivity between the primary application server(s) and the designated workstation from which it will be accessed
    2. A designated workstation/personal computer (PC) from which to work with the software
    3. Remote-access software to facilitate the connection (optional)

    With any of the following scenarios, the utmost care must be taken to ensure that the ECC's technology solutions for CAD, remote access, and network connectivity are implemented in the most secure way available at the time. For example, with remote workers, having a multifactor authentication requirement in place before access is granted can go a long way toward preventing cyberattacks.

| OPTION 1: *Backup Location* | OPTION 2: *Alternate Connected Location* | OPTION 3: *Remote Access to Workstations* |
|---|---|---|
| A fully functional backup location, including functional backup CAD stations, is the ideal scenario for remote work. This option meets conditions A and B above, and enables agencies to quickly decide to protect employee health and safety in the event of a primary ECC evacuation | With this option, an agency has already established an offsite location, such as a mobile command center, that satisfies conditions A and B above and is equipped with agency-owned workstations and connectivity to the network where the agency's CAD servers reside. This scenario, like a fully functional backup center, allows multiple employees to access the CAD system from a single site without the need to manage network connectivity for more than one location | In the event of a complete primary ECC evacuation, some staff members may need the ability to work from home to maintain the CDC's social-distancing guidelines and prevent the spread of viruses like COVID19. With this option, staff members would need to meet conditions A and B above from their remote location. From there, telecommunicators could access the CAD system by:<br>• Accessing and authenticating the remote workstation<br>• Launching remote-access software OR accessing the application installed on the workstation<br>• Connecting to a CAD workstation console at the ECC using remote-access software<br>• Authenticating credentials and logging into the CAD application |

With the first two options, it is assumed that network connections are secure and reliable, mitigating the risk of a cyber incident or attack. With the third, it is likely that staff members will have to use their existing consumer broadband connections, making it even more important to have a VPN in place. It also is assumed that users have access to workstations, whether in a backup location or at home, that have two screens to allow them to view the CAD application as it is intended by the developer.

3. **Dispatch.** Radio manufacturers and vendors offer a variety of remote dispatch solutions designed for public safety agencies. Each solution varies in its availability, functionality, and ability to be implemented quickly; however, it is possible to find a remote dispatch solution that will meet your agency's needs and budget.

| OPTION 1: *Portable Radios* | OPTION 2: *Control Station–Consolette* | OPTION 3: *Generic Dispatch Workstation* | OPTION 4: *Vendor-Specific Remote Dispatch Console* |
|---|---|---|---|
| In an area with reliable radio coverage, the use of portable radios is the recommended option for remote dispatch operations. While portable radios can be a cost-effective, easy-to-implement option for remote dispatch, there are some limitations, including single-channel operation and limited hands-free operation. In addition, agencies need to understand the condition of the radios and accessories, including batteries, chargers, and headsets. | With this option, dispatchers are provided with a mobile radio and power supply or a consolette. This option offers a more reliable radio link, as well as higher power output and a better antenna. It is also headset and footswitch capable and offers hands-free operation. | With this option, a generic workstation is set up using a remote PC or dispatch console to connect mobile radios or consolettes. This setup can control and manage multiple channels and offers hands-free operation, as well as headset and footswitch capabilities. Additional radios can be controlled with access to a broadband network. | This vendor-specific option gives agencies the ability to remotely access dispatch technology used at the primary ECC. Because it is vendor-specific, options may be limited, and it comes with a higher price tag than more-generic or universal options. A broadband network connection is required. |

Prior to implementing any remote dispatch solution, agencies need to consider some additional factors that could present a challenge in some or all the provided scenarios, including:

- Reliability of coverage in the area
- Radio programming for access to essential channels and/or talkgroups
- Dispatcher training on radios and consoles
- Broadband network access

## Conclusion

In a public-health crisis like the COVID-19 pandemic, agencies may be required to evacuate some or all of a primary ECC to protect staff, clean and disinfect the facility, and prevent the spread of illness. In some cases, an agency may have an existing COOP in place that outlines the steps to take to stand up a backup center or activate a secondary space like a mobile command center. While preplanning is important, and necessary, for ongoing operations, existing COOPs may not include provisions for protecting staff from the spread of viral illnesses or outline steps to take if fully or partially remote operations become necessary.

The scenarios outlined herein for remote call handling, CAD, and dispatch reflect just some of the options available to agencies finding themselves without access to their primary ECC. Ultimately, the options available to an agency for remote operations depend on the amount of preplanning that has been done and the budget available to transition operations. While some of the scenarios and options outlined here are not intended to sustain operations indefinitely, they can be used as stopgap measures to prevent extended interruption to operations as agencies plan and implement longer-term solutions.

## Resources

[1] What is Remote Work? RemoteYear.com: https://remoteyear.com/blog/what-is-remote-work

[2] NENA COVID-19 PSAP Checklist (v3): https://cdn.ymaws.com/www.nena.org/resource/resmgr/covid/COVID_PSAP_Checklist_v3.pdf

## About Mission Critical Partners

Mission Critical Partners is a professional services and network and IT support firm that helps clients enhance and evolve their public safety systems and operations through extensive experience, knowledge and resources. By providing insight and support every step of the way, we help our clients to transform their mission critical operations, maximize the value of their investments, and ensure optimal performance and success.

For more information, visit **MissionCriticalPartners.com**

Mission Critical Partners
690 Gray's Woods Blvd.
Port Matilda, PA 16870
Phone: 888.8.MCP.911 or 888.862.7911
Fax: 814.217.6807



April 2020 | Doc # OPSFACWP0420

MissionCriticalPartners