LEVERAGING THE PACE PLAN INTO THE EMERGENCY COMMUNICATIONS ECOSYSTEM

OVERVIEW

Maintaining operability, interoperability, and continuity of emergency communications is critical for emergency response regardless of the operating conditions. Primary, Alternate, Contingency, Emergency (PACE) communications plans are a tool for helping organizations prepare for backup communications capabilities in out-of-the-ordinary situations. PACE planning helps organizations establish options for redundant communications capabilities if primary capabilities are disrupted or degraded.

It is critical for communications to continue despite disrupted communication networks. Perfect situational awareness is not always possible, and communications may be impacted by environmental factors affecting infrastructure, equipment, and users. The PACE concept takes redundancy beyond the typical planning of having a primary means and a backup. A PACE plan is triggered when the primary capability becomes unavailable.

A PACE plan helps organizations establish predictable and redundant communications capabilities in changing operational environments. Having redundant communications methods in place and sharing these among users helps achieve interoperability and continuity throughout the emergency communications ecosystem, particularly in challenging environments.

GROUNDWORK

Building an effective PACE plan is a challenging task. The key to a good PACE plan is to establish redundancy among the communications capabilities available, so that some means of communication is always made available. Organizations need to ensure their proposed PACE plans are feasible, acceptable, suitable, distinguishable, and complete.

- **Feasible.** Have enough working systems and trained users to implement each step of the PACE plan for both transmitting and receiving users
- **Acceptable.** Setting up a redundant capability must not interfere with operations or other continuity of operations activities that may be occurring simultaneously
- **Suitable.** Redundant capabilities must have the capacity to meet operational requirements
- **Distinguishable.** Redundant communications cannot rely on an impacted method. For example, if network data is not available, Voice over Internet Protocol would be a poor backup method. If VHF radio communications are degraded or denied, the next step in the PACE plan should use a different transmission medium
- **Complete.** The PACE plan should outline each means of communication, and triggers for execution

In order to build an effective PACE plan, planners must identify all the potential essential functions of a particular mission, understand their organization's authorized and available communications capabilities and limitations, and adhere to the personnel and logistical requirements to employ and sustain the capabilities.

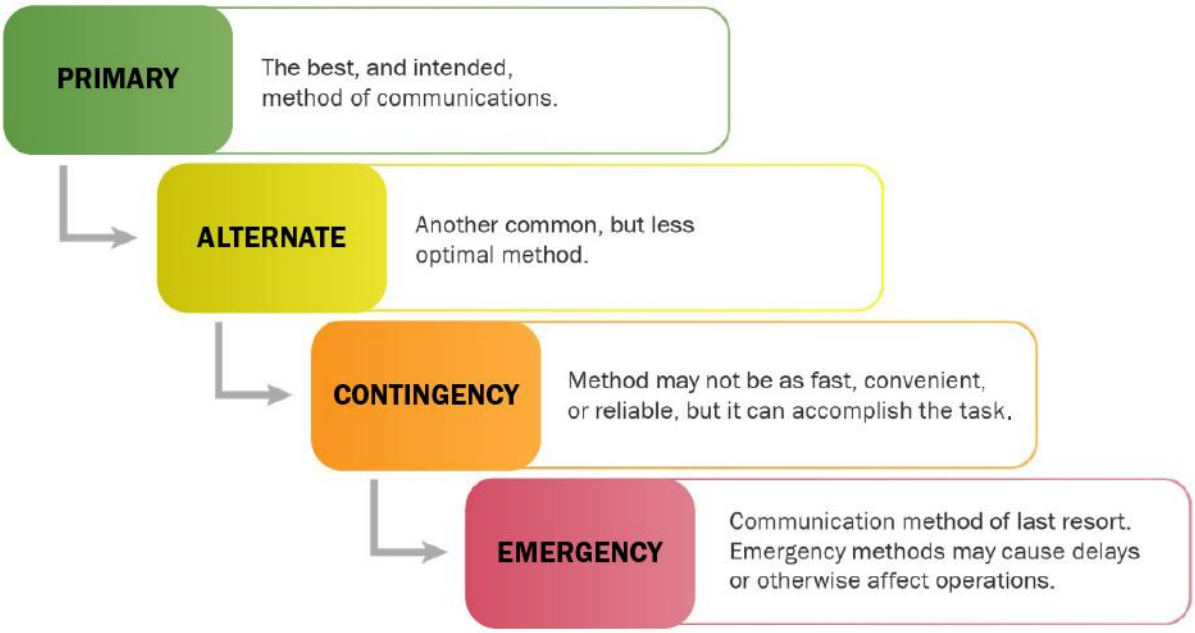
DEVELOPING THE PACE PLAN

The PACE plan should be as simple as possible to support reliable communications during dynamic operations. Alternate communications methods in the plan should ensure communications availability, and users should be comfortable with those systems if the primary means of communication fails. Public safety organizations should practice the PACE plan during training and exercises to ensure all personnel can execute the plan as necessary.

PACE planning helps organizations establish an order to deploy communications assets when capabilities are disrupted or degraded. The **Primary** level is a typical day-to-day method of communication. **Alternate** is the backup to the Primary. **Contingency** is used if both Primary & Alternate have failed. **Emergency** is the fourth level if all other levels are not working.[1] A PACE plan moves from level to level based on failures of the current communication mode. Additionally, a plan for communications failures is good practice for critical missions.

Planning includes evaluating possible points of failure for each proposed method and identifying the most reliable within anticipated locations and environments of operations. For example, listing email, Facebook, and texting as three levels of the plan are of no value if they depend on the same device and communications path, i.e., cellular data. The same communications path or method should never be used more than once. A nonfunctional method or path has no value in the progressive steps of a PACE plan.

PACE planning should take into consideration both outgoing communications and commonly available incoming methods of receiving communications. Outgoing and incoming communications may be impacted by the location of the originating message and the destination for the communication. No matter how common a form of communication may be, if a geographic area negatively impacts the ability of certain communications nodes to transmit or receive messages, then another should be chosen for a PACE plan. Alternatively, a PACE plan may need to specify a location outside of the operation's geographical area as a reach-out point.



[1] *FM 6-02 Signal Support to Operations* (Headquarters, Department of the Army, September 2019).

CONSIDERATIONS

User: For the sender and recipient of the message, progression through PACE usually goes from simple to more complex. If the normal method is to send an email, and the Alternate is to call on the phone, the recipient may need to write information down, and then transfer it into a digital format at the receiving end. If it progresses to a Contingency level the sender may need to write the message out, hand it off to another individual to transmit the message, the receiver may need to write the message down, and then deliver it to the recipient. If it gets to the Emergency level, it could involve using a runner to pick up the written message and travel to the recipient's location to deliver it.

Technology: Technology usually goes from complex to simpler options, relying on less technology as it progresses, while hoping to improve the reliability. As the situation advances through the levels, the amount of information that can be transmitted will likely decrease. For instance, the user can send attachments through email, such as photos, documents, etc. Using an audio communications method reduces the user to information that can be exchanged verbally. If the plan includes High Frequency (HF) radio such as auxiliary communications or Shared Resources (SHARES), data rates will be limited compared to primary paths.

Cybersecurity: Like any risk to communications operability, interoperability, and resiliency, cybersecurity must be considered for communications modes using Internet Protocol-reliant technology. Cybersecurity hygiene of system users and proper upkeep of available cyber protections for systems must go hand-in-hand with an organization's PACE plan.

Time: Time will also be a factor as the situation moves past the primary communications methods. The time required to transmit a message will increase as more steps are added to the process. Time may also be a factor in implementing backup capabilities. As you get to the Emergency means of communication, you may need certain personnel to operate backup equipment. If not staffed 24/7, your planning will need to consider the time needed to bring in additional or specialized staff. As the situation shifts throughout the levels, there will be a need to adjust the ways you operate in order to account for inoperable or disrupted communications methods. As the user complexity increases, the length of time required to get messages through increases.

Quality: If a user becomes more limited in the volume of information that users can send, their messages will need to be more concise, formal, and structured. In Primary operation, a quick return phone/radio call or email to ask a clarifying question happens all the time. When it reaches the Contingency and/or Emergency level and messages are taking significant time to move back and forth, sent messages that require clarification will delay critical action. The sender will need to use more formal methods such as specific forms to ensure that requestors send all the needed information the first time.

Developing a PACE plan is a collaborative effort involving operational procedures and communications options. For instance, if a plan solely accounts for the technical side, it will not always consider the impact to users and the functions that will need to be adjusted. When a plan just considers the operational side, it may not account for all the impacts, limitations, or technical details required to implement the planned backups. Thus, it is critical to have subject matter experts involved in developing the plan who can address the technical, operational, and administrative considerations of each level's capabilities. There are additional factors to consider within the PACE plans. Planning should include overarching interoperability, possibly on the state level, and a separate PACE plan for local entities. Also, planning for the possibility of no communications should be addressed. In some cases, there may not be resources to implement all four means of communications and the Emergency means may need to be considered as no communications.

PACE TRIGGERS

Once the planners identify and establish the framework of the PACE plan, the next step is to determine the trigger points that would initiate an organization to switch from Primary to Alternate, from Alternate to Contingency, and from Contingency to Emergency. For instance, if a primary cyber system fails, agencies should be prepared to use Alternate, Contingency, or Emergency systems while the Primary system is being restored. In order for an agency to run smoothly despite disrupted communications, it is essential to identify points of failures and decide how and when to move to the next level of the PACE plan once failures of the current mode are confirmed.

TRAINING AND EXERCISES

The individuals who will operate the Alternate, Contingency, and Emergency means of communications will need regular training and experiences using these systems. Exercises and practicing your organization's PACE plan not only reinforce that training but identify issues and leads to improvements. Public safety organizations that understand and practice cascading failures will likely be more resilient when faced with other out-of-ordinary situations. Hopefully organizations never need to use these emergency plans, but the process of building a plan, training, and exercising will help maintain emergency communications capabilities.

CONCLUSION

Developing and implementing a PACE plan improves an organization's emergency communications preparedness for out-of-the-ordinary situations. Achieving optimal operability, interoperability, and continuity outcomes through PACE planning helps ensure communications and information sharing systems meet public safety's mission-critical needs.