


GovGram is a multi-communication notification system designed to allow public agencies to quickly and efficiently communicate with residents. Beyond your typical “Reverse 911” system, GovGram utilizes state-of-the-art technology coupled with a MS SQL backbone to deliver both emergency notifications and community announcements.


All personal information is securely hosted on a dedicated server at a *tier one* hosting facility. The server is housed in a different time zone and located on a separate power grid. This level of security and multiple backup redundancies allows our clients to confidently initiate emergency notifications during a crisis. (see [Secure Hosting](#))



**Two Types of Communication**

- Emergency Notifications
- Community Announcements

**Three Methods of Communication**



- Voicemail Broadcasts
- Text Messages
- Email Notification

### Emergency Notifications:

- Does not require each resident to register
- Emergency notification database provided by Verizon
- Verizon database consists of:
  - > Residential land lines for every land line carrier
  - > Business land lines for every land line carrier
  - > Listed and unlisted telephone numbers for every land line carrier
- Verizon database updated weekly
- Reverse GeoCoding: **New Feature**
  - > First responders can now draw a polygon over a web-based map to select specific areas for targeted communication

### Community Announcements:

- Residents register and opt in via a web-based portal
- Residents manage communication preferences via a secure, “My GovGram” page. Preferences include:
  - > Opting in to receive community announcements
  - > Changing personal contact information
  - > Selecting the method of communication

## **GovGram Hosting**

Our data centers are engineered to the standards required to support a Zero-Downtime Network™. They are designed and maintained without compromise for security or redundancy.

### **Physical Security**

- Keycard protocols, biometric scanning protocols and round-the-clock interior and exterior surveillance monitor access to every one of our data centers.
- Only authorized data center personnel are granted access credentials to our data centers. No one else can enter the production area of the data center without prior clearance and an appropriate escort.
- Every data center employee undergoes multiple and thorough background security checks before they're hired.

### **Precision Environment**

- Every data center's HVAC (Heating Ventilation Air Conditioning) system is N+1 redundant. This ensures that a duplicate system immediately comes online should there be an HVAC system failure.
- Every 90 seconds, all the air in our data centers are circulated and filtered to remove dust and contaminants.
- Our advanced fire suppression systems are designed to stop fires from spreading in the unlikely event one should occur.
- All cables are securely tied down with cable racks suspended from ceilings, providing dual routes for all cables.

### **Conditioned Power**

- Should a total utility power outage ever occur, all of our data centers' power systems are designed to run uninterrupted, with every server receiving conditioned UPS (Uninterruptible Power Supply) power.
- Our UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails.
- If an extended utility power outage occurs, our routinely tested, on-site diesel generators can run indefinitely.

### **Core Routing Equipment**

- Only fully redundant, enterprise-class routing equipment is used at our data centers.
- All routing equipment is housed in a secured core routing room and fed by its own redundant power supply.
- Fiber carriers can only enter our data centers at disparate points to guard against service failure.

## Reverse Geo-Coding

Reverse Geo-Coding utilizes state-of-the-art GIS (Global Information Systems) technology. Once activated, this embedded technology directs into you into your administrative control panel.

By utilizing reverse geo-coding, authorized users can pin point exact locations for targeted emergency communications. Reverse Geo-Coding would be utilized in the event of an isolated incident that only requires a notification to a particular geographic location.

For example:

A water main breaks on the Northeast section of the municipality and only an alert is sent to that area.

