WHITE PAPER

What does it cost to build an in-house Public Warning Service front end?

The True Cost of “Do It Yourself” (DIY)

Public Warning Service (PWS) are systems which government and public authorities use to alert the public (residents and visitors) of imminent and developing major emergencies and disasters. Such alerts or warnings may be transmitted to the population through a variety of modalities including:

PUBLIC WARNING TRANSMISSION

- **alerts to mobile phone users**
- **mobile apps, email, SMS, voice calls, social media posts**
- **sirens, radio, tv, social media, TETRA, digital signage, and opt-in address based systems.**

The European Union considers the protection of Europeans and anyone visiting the region a top priority. To ensure that all member states are prepared to alert citizens and respond to any public safety incident, emergency, or disaster in a targeted, fast, and reliable way, the EU Directive EECC Article 110 requires all European Union and European Economic Area countries to implement a PWS using mobile network communication channels by June 2022.

What Constitutes an "EU Approved" PWS?

The mandate requires that all member states "ensure that, when public warning systems regarding imminent or developing major emergencies and disasters are in place, public warnings are transmitted by providers of mobile number-based interpersonal communications services to the end-users concerned." The regulation explains that "end-users concerned should be considered to be those who are located in the geographic areas potentially being affected by imminent or developing major emergencies and disasters during the warning period, as determined by the competent authorities."

In summary, an "EU approved" PWS under EECC Article 110 mandates that member states be able to do the following:

- Define the affected geographic area and identify end-users to prevent widespread panic,
- Convey alerts or warnings in real time, rapidly and reliably,
- Reach as many people as physically possible within that targeted area, including citizens, residents, visitors, and inbound roamers,
- Send mobile-number based communications without the need for people to register, opt in, or download any mobile app, or configure their mobile phones,
- Automatically inform people of the existence of such a public warning system as they enter the affected area or the country.

What Options do Governments/Member States Have?

The modern PWS is comprised of a back end and front end.

On the one hand, the back end is the technology and equipment installed within the telecommunication providers' infrastructure to enable the transmission of direct messages and alerts to residents and visitors. Previously done with traditional PWS (sirens, radio, TV), modern PWS can send alerts directly to mobile phones based on geographical locations. This can be achieved by two underlying technologies:

- Cell Broadcast (CB) is a method of sending messages to multiple mobile telephone users in a defined area at the same time. This is also known as Short Message Service-Cell Broadcast (SMS-CB).
- Location-based SMS (LB-SMS) is a technology which uses the Telecom Operators' Infrastructure to send normal SMS, directly to the network's attached mobile devices, which happen to be in a defined geographical area.

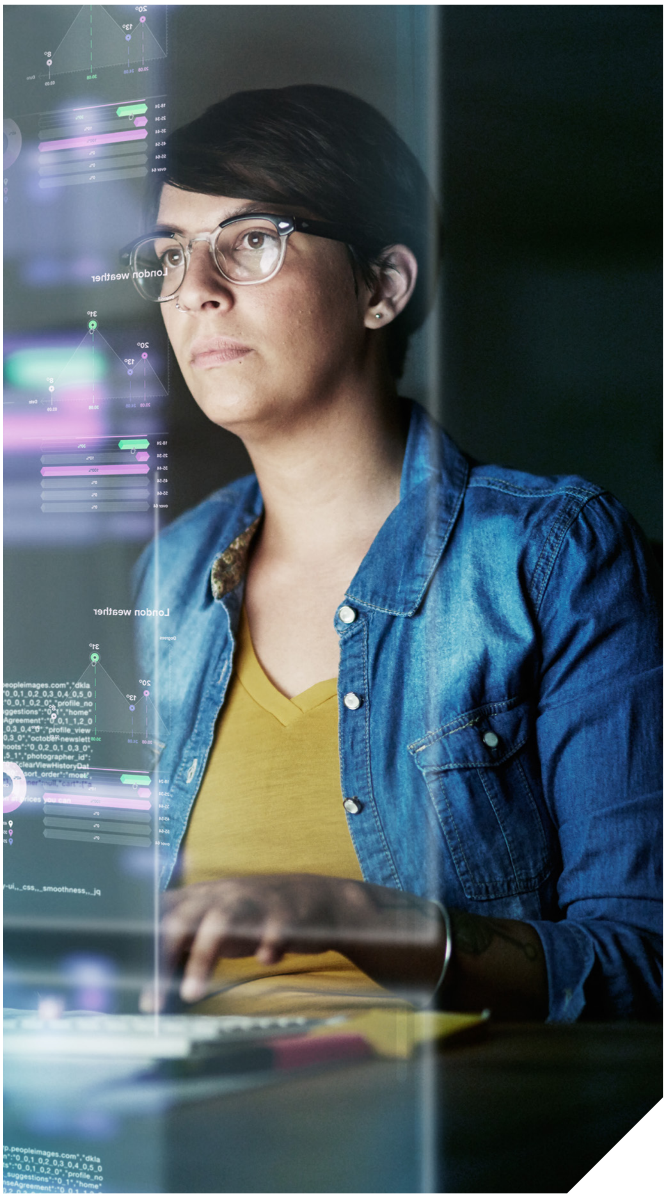
It is important to note that although these messaging standards are supported within the mobile networks it will still require specific equipment to be installed and integrated within the telecommunication providers before a CB or LB-SMS service can be offered to subscribers.

On the other hand, the public alerting front-end consists of the consoles (user interfaces), messaging gateways, and orchestration logics which public authorities use to compose messages, select communication channels, and send alerts to the maximum number of people in a geo-targeted area ranging in size from a localised residential area, city, or state, to an entire country.

In 2020, the Body of European Regulators for Electronic Communications (BEREC) issued guidelines on how to assess the effectiveness of PWS transmitted by different means.

To comply with the EU directive according to the BEREC guidelines, member states must:

- Select a back-end communication technology for sending alerts to mobile phones or use a combination of cell broadcast and location-based SMS messaging
- Select a public alerting front-end gateway provider or engage in a software development project to build one, known as "Do It Yourself" (DIY)



What Does it Really Take to Build an In-House Public Warning Front End?

In-house software development or DIY refers to the choice made by an organisation to manage the entire creation process using in-house resources or a third-party vendor like a system integrator or technology services company. In this case, governments or public authorities accept the massive development challenge and the cost of hosting, supporting, and maintaining the system. More often than not, the complexity of building a front end is underestimated.

Building an EECC-compliant, reliable, and economically viable PWS may typically require more than just contracting a system integrator and funding a development team for a few years. Considerations of in-house experience and competency as well as long-term availability and reliability of resources are needed for any software development project built 100% in house, or in collaboration with consultants. Usually such an approach requires highly skilled staff internally who have the capabilities to build a robust and future-proof system to meet the EECC requirements for public alerting.

An equally important consideration is the evolution of the system. The scope required to meet the EECC requirements might seem manageable from a custom development perspective; however, for many countries this scope will only be the starting point for a national system that will potentially be used for many different alerting scenarios in the future. A system must therefore satisfy some key capabilities of expandability and roadmap evolution. For example, it is very likely that additional communication channels will be added in the years after the initial deployment. Supporting more advanced alerting scenarios where communication channels are combined may be required, and additional EECC requirements related to two-way communication may come in the future.

IN-HOUSE DEVELOPED SOLUTION COSTS CAN INCLUDE:

- Project management cost (direct or through system integrator)
- Project team hiring, sub-contracting costs, salaries, and benefits
- Facilities, personal computers, development tools
- Technical infrastructure, hardware
- Development, Q&A and production environments
- Telecommunication

Here's a breakdown of upfront costs:

- Developing the front-end solution. National public agencies responsible for public safety, civil defense, and crisis management assemble internally or sub-contract a team comprised of software architects, a developer, mobile app developers, database administrators and at least one User Experience (UX) designer who ideally has experience and expertise in telecommunication technology and equipment, GIS mapping, APIs, and overall integration. Along with the developers, team members from quality assurance, security information, project management, and DevOps resources will also be required to conduct the project to completion. Besides resources, you will need to account for the tools, software licenses, different technical environments (dev, staging, production), the communication and collaboration tool, the project management tools, as well as the required office space.
- Integrating the front end with the back ends. The front end integrates with all and any types of back-end technologies (cell broadcast, location-based SMS, or a combination) which are hosted with the telecom operators' networks. This is a development project which will require very specific technical skills, where experience in integrating with generic APIs is not enough. You will need to work with software engineers who understand the technological possibilities and limitations on the "inside" of the telecom networks, specifically all the bits and pieces needed to send alerts to a specific geographic area. This also includes the ability to send messages to certain base stations, and therefore understand the differences between cell broadcast technology versus SMS, among other considerations.

Some operational budget must be reserved to cover the cost associated with hosting, operating, monitoring, supporting, and maintaining the solution over time. It's important to pay special attention to sizing, especially for the hardware component, in case the development and delivery are done in-house by a team with limited experience with these systems. It is likely that the hardware dimensioning will be either excessive, or actually under-dimensioned.

- Hosting the front-end solution. To account for the hardware, the databases, the different environments— dev, test, prod— and the software, you'll need to build, test, and run the solution in the production environment. Will it be on-premise or hosted in the cloud? There are many questions which must be answered upfront and which will have an impact on the overall budget. It will likely need a multi-tenant system, or at least support different types of organisations and user roles with a flexible setup for controlling user rights, alarm sending approval logic, and secure access. Because the solution must be highly available, you'll want to consider active-active clustering with fully geo-redundant configuration or the use of a disaster recovery site.
- Monitoring the solution. The front-end solution will most likely be flagged as a mission critical application by your IT ops teams and will require 24/7 support and monitoring by the NOCs along with a runbook and an escalation procedure in case of a problem. This is a Catch 22, because when something wrong happens with your brand-new population alerting tool, authorities will not be able to reach out to the population at risk during critical events. This is exactly what happened during the terrorist attack a few years ago on the French national day in Nice, France, causing many casualties and general chaos. Such systems must have very robust features for continuously monitoring the integrated channels and must have contingency capabilities to make sure faults are handled. Further, the system must be able to support simulations and semi-simulated scenarios for test and readiness purposes.
- Communicating with residents and visitors. Besides text and/or SMS, will authorities want to transmit alerts via additional channels? For instance, is a mobile app push notification a requirement? Again, this would be yet another development project which would require human and technical resources for design, development, hosting, support, maintenance, and a budget to cover it all.
- Supporting the tool. You will need to provision for all of the support functions necessary to operating the solution. What happens when there is bug or a computer glitch which prevents the front-end application from transmitting alerts? This can be a big undertaking for systems needing 24/7 support with strict SLAs (response and repair times) where also 3rd line support with access to developers with in-depth knowledge of the system code base and configuration will be needed.
- Time to value. Like any IT solution development project, the time to readiness will depend on many factors including resource availability, hardware and tools, budget, and project management.

Embarking on an in-house development project for building a Public Warning alerting gateway, or using a mix of in-house resources, consultants and vendors without proven products and experience, can quickly become very expensive and time consuming, and presents higher risks in terms of project failures and critical project delays.

What is the Alternative to DIY?

Protecting the population is a critical challenge and top priority for most governments and countries. Public officials responsible for public safety will not be forgiven if they fail. In this context, building a front-end solution from scratch can be a very risky decision not only from an economic perspective but also from a political one. The alternative is to remove this risk by partnering with a company that has already built government solutions for public warning and has years of experience helping countries respond to the most catastrophic events and pandemics.

There are several Public Warning solutions available out there with different deployment options, such as:

- Modular approaches offering the front-end alerting gateway only, a specific type of back end only, or both front end and back end components,
- Basic solutions, or more sophisticated combinations of capabilities,
- A single product, or a platform which can be expanded to include many communication channels.

There is therefore a large and customisable variety of solutions to choose from which address the current and future needs of member states. In addition to providing ready-to-use solutions, public warning solution vendors take responsibility for the support and maintenance of the solution and will guarantee service levels to give you the assurance of maximum availability.

There is a distinct set of PWS vendors with full end-to-end offerings including in-depth knowledge of the telecom systems (including cell broadcast platforms and location-based SMS platforms), the front-end alerting gateways, multi-channel gateways, and alarm centers.

Whether the scope of the national project is limited to the compliance of a regulation such as the EU/EECC directive Article 110, or the implementation of a more sophisticated solution, working with experienced vendors in the Public Warning space offers key advantages such as reducing the time to value. Because these systems come "pre-integrated" and ready-to-use, there is no need to spend extra time or resources building the different components and maintaining the system for years to come. Most likely, the systems are proven and have already been used by other countries before, during, and after critical events.

How Should Member States/Governments Decide Which Solution is Best?

Member states, countries, and other governmental departments exploring the possibility of an in-house front-end alerting gateway should carefully assess the amount of resources and skills available and budgets allocated to the project. It is important to consider the total life cycle of the system and to consider that the initial scope and project is most likely only the starting point. From a delivery perspective, a retro-planning must be created to ensure the project timeline, and ensure the risks associated with potential delays are well understood so that the solution can be built, tested, deployed, and maintained prior to the EU directive deadline of June 21st 2022.

Keep your people safe. Reach and communicate with millions in seconds. Learn more:

https://everbridge.co.uk/products/public-warning/

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company providing enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,000 global customers rely on the company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans.

The company's platform sent over 3.5 billion messages in 2019 and offers the ability to reach over 550 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Australia, Greece, Iceland, the Netherlands, Peru, Singapore, Sweden, and a number of the largest states in India.

The company's critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement™ and Secure Messaging.

Everbridge serves 8 of the 10 largest U.S. cities, 9 of the 10 largest U.S.-based investment banks, 47 of the 50 busiest North American airports, 9 of the 10 largest global consulting firms, 7 of the 10 largest global auto makers, all 4 of the largest global accounting firms, 9 of the 10 largest U.S.-based health care providers, and 6 of the 10 largest technology companies in the world.

Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Abu Dhabi, Beijing, Bangalore, Kolkata, Paris, London, Munich, New York, Oslo, Singapore, Stockholm and Tilburg.

For more information, visit www.everbridge.com.

everbridge®

VISIT www.everbridge.com/products/public-warning/
EMAIL publicwarning@everbridge.com
CALL +44-(0)800-035-0081