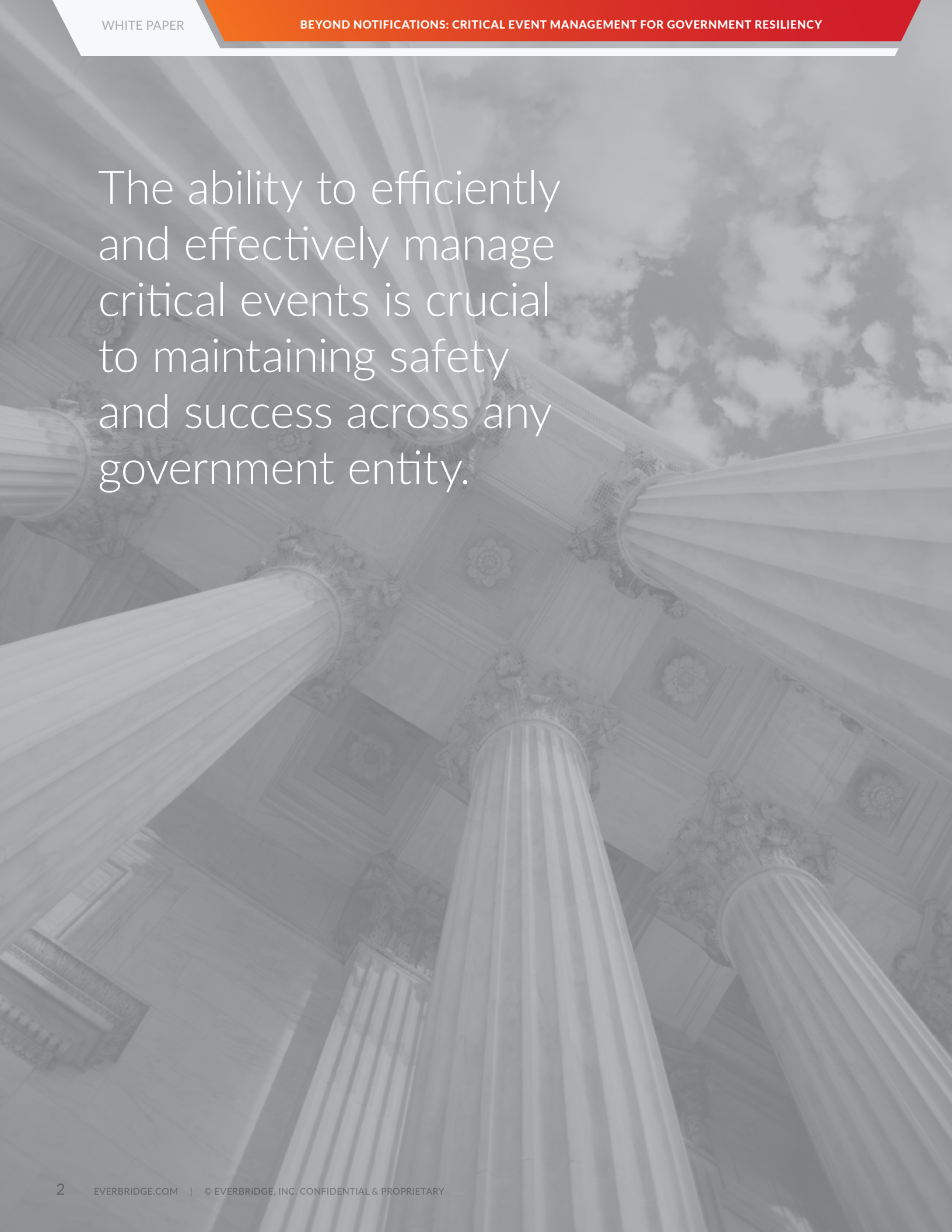


A small blue icon of a document with three horizontal lines.

WHITE PAPER

# Beyond Notifications

CRITICAL EVENT MANAGEMENT FOR  
GOVERNMENT RESILIENCY



The ability to efficiently and effectively manage critical events is crucial to maintaining safety and success across any government entity.

In today's complex threat climate, critical events come in both physical and digital forms. As we experience an increase in active shooter situations, terrorist attacks, severe weather conditions, IT outages, and cyber-attack incidents an agency's ability to act quickly and appropriately is vital.



CEM, or Critical Event Management, encompasses mass notification within a more holistic strategy.

Having a reliable and scalable system in place that allows governments to strategically manage the entire lifespan of any and all threats is invaluable. However, according to the MIM Annual Report, 73% of respondents felt that their companies either did not invest or did not invest enough into Major Incident management. An organization's ability to successfully manage critical events, both physical and digital, is greatly enhanced through investment in technology.

Implementing technology that automates incident response serves to increase an organization's operational resiliency and business continuity. The first step many agencies take toward successful management of critical events often begins with deploying an Emergency Mass Notification System (EMNS). While mass notification is a key component in keeping your people safe and your operations running efficiently, an EMNS is just the first step toward ensuring maximum operational resiliency.

CEM, or Critical Event Management, encompasses mass notification within a more holistic strategy.

A complete CEM strategy ensures optimal safety and security standards are met while increasing an agency's ability to maintain operations during disruptions. CEM addresses the entire lifespan of a critical event, rather than being a singular tool that is only used at the time a critical event is occurring. CEM enables government entities to manage the before, during, and after of any disruption.

While a complete CEM strategy is the ultimate goal in enabling maximum resiliency against disruptions, it must begin with solid foundational work. This requires agencies to establish a working mass notification system in order to go beyond just notifications. Successful implementation of an EMNS allows governments to enable expansion of their capabilities and work toward unlocking a fully integrated and automated approach to critical event management.

## Establishing a Solid Foundation with Mass Notification

### INTEGRATION WITH PERSONNEL SYSTEMS

The importance of seamless integration between your personnel systems and your EMNS cannot be understated. Prior to deploying an EMNS, be sure integration between the two is possible to avoid information silos that can lead to ineffective communication and potentially costly or dangerous errors.

Employee location data must be able to flow into your EMNS to enable optimal alerting capabilities, allowing messages to be sent to people in affected areas. If this flow is blocked or sending through outdated or incorrect information, your notifications will not reach the appropriate personnel and consequently render any EMNS meaningless.

This means HR systems not only require interoperability with your EMNS, but also the maintenance of up-to-date information on the status and geo-location of all current employees. Understanding your mass notification capabilities are only as good as the information you supply the system is crucial during deployment.

Furthermore, your systems should be able to capitalize on horizontal integrations across agencies. This will allow the system to dynamically track employees and continue to properly notify them should they change statuses or move to a different agency.



Employee location data must be able to flow into your EMNS to enable optimal alerting capabilities, allowing messages to be sent to people in affected areas.

### ACCURATE GEO-LOCATION AND ACCESSIBILITY OF YOUR PEOPLE

Reaching employees in government and federal spaces requires accurate geo-locations and accessibility to employee devices. It is important to select a platform on an unclassified system that is able to reach employees outside of their defined facilities.

A prime example of this was experienced during the pandemic. In the wake of shelter-in-place mandates, agencies were forced to maintain operations even as massive amounts of non-essential employees were suddenly required to work from home. These employees were without classified systems, however, they still needed to be quickly and accurately alerted.

Looking forward, a successful deployment of an EMNS for government and federal spaces must facilitate an unimpeded flow of geo-location data while being on an unclassified system. This enables your organization to know exactly where to send alerts with the confidence they will reach the intended recipient.



From vendor selection to implementation responsibilities, it is important to know you are working with experts who understand the intricacies of government and federal agencies.

## EXPEDITING IMPLEMENTATION AND ONBOARDING

In order for your EMNS to work for you, it first has to be up and running. To expedite this process, the right people need to be involved. From vendor selection to implementation responsibilities, it is important to know you are working with experts who understand the intricacies of government and federal agencies. Not all solutions are interoperable in these spaces, so first ensure the EMNS you purchase has been successfully deployed in other government and federal spaces and is FedRAMP certified.

Second, make sure the correct people in your organization are trained to use this tool in the right way. When you make the decision to purchase an EMNS, look at the customer support network. Ask if there is a technical assistance manager available, even if for a limited amount of time, to bring your team up to speed while providing training that will allow your current team to train future members quickly and successfully as well.





## **AUTOMATION FACILITATES EASE OF USE, INCREASES ACCURACY, AND REDUCES NOTIFICATION FATIGUE**

It goes without saying that timeliness is everything when dealing with critical events. Your EMNS needs to provide intel and facilitate response to events as they happen, so your organization can act appropriately and immediately if need be. Automation is one of the main factors that contribute to a successful EMNS deployment, especially for government and federal environments.



Automated up-to-date employee data coupled with real-time intel creates highly accurate messaging that reduces the agency's reliance on any singular employee.

### **Ease of Use and Accuracy**

When looking for an EMNS, understand how automation can assist an agency's ability to manage critical events as they occur. Automation not only introduces speed of response time, but also creates an easier user experience. Through automation, the number of decisions an employee needs to make is drastically decreased. This leads to less stress on the employee's end and an increase in willingness to engage with the EMNS tool in the future.

The ability to pre-define rules and scenarios for when and what the EMNS should be alerting on allows the system, rather than an employee, to decide if a mass notification is required. Furthermore, as the system is automatically being fed employee status and geo-location data, it already knows the affected parties and exactly to whom the notification should be sent. Automated up-to-date employee data coupled with real-time intel creates highly accurate messaging that reduces the agency's reliance on any singular employee.

Your EMNS needs to provide intel and facilitate response to events as they happen, so your organization can act appropriately and immediately if need be.



When individuals are inundated day after day with mass notifications from their organization, they begin to treat every message the same and often these messages go ignored.



In addition to a mass notification going out to impacted employees, an EMNS should also notify senior leadership.

### **Reduction of Notification Fatigue**

A system's ability to dynamically determine the appropriate recipients for a notification helps employees to be more selective, only using the system to send highly relevant information. This ensures people pay attention when a notification is sent to them, increasing the rate of response.

When individuals are inundated day after day with mass notifications from their organization, they begin to treat every message the same and often these messages go ignored. You never want your alerts to be dismissed, especially when about time-sensitive events.

Your organization needs to determine what notifications should be an all-employee blast, a regional blast, a highly local blast, etc., and this information needs to be part of your EMNS automation. Furthermore, find out if your EMNS has separate systems for various alerts. This can even further reduce notification fatigue.

### **Automated Internal Notifications**

As you build a critical event management program in your agency, your EMNS should be a key part of your escalation protocol. In addition to a mass notification going out to impacted employees, an EMNS should also notify senior leadership.

It is not enough to send mass notifications to the appropriate employees in the affected area. Your agency probably has protocols in place that require certain executives to be advised of any adverse actions incurred by the agency. Having an EMNS with automation in place, allows notifications to be automatically generated so that specified executives, as well as any crisis response group in your agency, are provided information in real-time.



Whatever gaps your organization identifies, a solid EMNS will give you the confidence to begin taking the necessary steps toward implementing an end-to-end critical event management platform.

## Mass Notification is the Foundation for a Complete Critical Event Strategy

Implementing an EMNS allows federal spaces to fulfill their duty of care to employees, maintain streamlined communications that ensure business continuity, and remain efficient during critical events.

However, while an EMNS is a tool that adds incredible value to your organization, it should only be the first step in developing a cohesive critical event management strategy. This is why it is imperative that initial deployment of your EMNS is successful.

A successful deployment of an EMNS will highlight what else your organization needs to successfully manage a critical event. For example, while you now have notification capability, you may realize you need more advanced intel on potential critical events flowing into your EMNS. Or, perhaps your agency requires further assistance to immediately identify where potentially impacted people, facilities, and assets are located in order to send highly relevant alerts.

Whatever gaps your organization identifies, a solid EMNS will give you the confidence to begin taking the necessary steps toward implementing an end-to-end critical event management platform. Full integration and technology that houses all intel in one centralized location increases your ability to appropriate respond when a critical event occurs.







Automation serves to increase a government or agency's efficiency, while providing richer intelligence and correlation of threats with locations of assets and people.

## The Power of a Critical Event Management Platform in Government & Federal Spaces

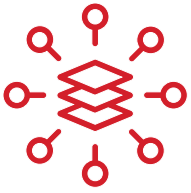
### WHY CEM?

In order to ensure maximum organizational resilience that will keep your people safe and your operations running efficiently, implementing a CEM platform is the key. Why?

CEM platforms automate manual processes. Automation serves to increase a government or agency's efficiency, while providing richer intelligence and correlation of threats with locations of assets and people. This ensures a more rapid and comprehensive incident assessment and remediation.

Furthermore, between rising information-security and cyber-attacks, business application slowdowns, IT service disruptions or interruptions and unpredictable man-made errors, it is not a question of if, but when, a serious outage or performance issue with your digital infrastructure will endanger the health of your operations and the communities you serve.

To address these challenges, CEM platforms help governments and agencies manage, control, and automate their operational response to resolve incidents faster, and ultimately ensure resilience for the future.



As you begin to conduct research on the best CEM platform to carry out your government or agency's automation, make sure it not only checks surface level requirements, but is reliable, scalable, secure, and provides exceptional support.



Does the messaging platform meet even the strictest security standards required in your industry and geographic markets?

## FOUR ESSENTIAL REQUIREMENTS FOR POWERING A CEM PLATFORM

It's easy to find a critical event alerting and management solution that, on paper, ticks all the features and function boxes. But none of those features will do any good if they aren't available, without delay and without fail, to facilitate the communication, collaboration and orchestration you need to respond to anything from an IT outage to a natural disaster or safety crisis.

That's why, in evaluating a CEM solution you need to look for whether the underlying platform has the following four essentials to ensure your operational response automation system is in fact up and operating even under the worst circumstances.

That's the only way to be sure you can quickly engage with the right responders, and notify the thousands, hundreds of thousands or millions of people affected by an emergency.

The four essential requirements for the platform powering your operational response automation system are:

### Reliability

Will your messages reach everyone who needs them, as quickly as required, regardless of the recipient's location or the failure of one or more communication channels? Has the messaging platform, or the provider, examined every communication link and eliminated every foreseeable weakness? What are the agreed service levels and is compliance with them audited by a trustworthy outside partner?

### Scalability

Can the underlying message platform quickly scale to meet even the sudden, unpredictable surges in demand caused by multiple simultaneous critical situations while meeting its uptime and performance commitments? How large an enterprise can the provider support?

### Security

Does the messaging platform meet even the strictest security standards required in your industry and geographic markets? Is the platform provider proactively working to meet future security requirements in every vertical and geography in which you operate? Can they prove their compliance?



Does the provider offer support not just for the technical operation of the platform, but ongoing education and consulting for its proper use?

### Support

Are both technical and customer support for the platform available with the same 24/7/365 assurance as the messaging service itself? What does 24/7/365 really mean? Does the provider offer support not just for the technical operation of the platform, but ongoing education and consulting for its proper use? Do they offer a “last resort” option to create and send messages even if all your communications and infrastructure are unavailable?

As you begin to conduct research on the best CEM platform to carry out your government or agency’s automation, make sure it not only checks surface level requirements, but is reliable, scalable, secure, and provides exceptional support.



When selecting a vendor, consider if they possess the ability to successfully deploy at the scale required for your organization.

### SELECTING A VENDOR: SCALABILITY, SCOPE, AND EXPERTISE

When selecting a vendor, consider if they possess the ability to successfully deploy at the scale required for your organization. Further, ensure your vendor can check off the following when it comes to due diligence:

- + Are they FedRAMP certified? If not, government agencies cannot use the solution.
- + Do they have demonstrated expertise and experience to ensure successful deployment?
- + What is their uptime rate? The difference between even 99% and 99.999% is huge when an urgent notification needs to get out.



## Let’s Talk

If you would like to discuss more about how a CEM platform will help your government or agency, please reach out. Everbridge is FedRAMP certified and is experienced in the requirements necessary for integration into government and federal spaces. We are here to help with any questions you may have. Get in touch or just call us at +1-818-230-9700 to learn more.

# About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications for automating and accelerating an organizations' operational response to critical events in order to Keep People Safe and Organizations Running™. During public safety threats such as active shooter situations, terrorist attacks, a global pandemic 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 5,800 global customers rely on the Company's Critical Event Management (CEM) 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 modalities, and track progress on executing response plans. 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, 8 of the 10 largest global automakers, 9 of the 10 largest U.S.-based health care providers, and 7 of the 10 largest technology companies in the world. Everbridge is based in Boston with additional offices in 25 cities around the globe. For more information visit [www.everbridge.com](http://www.everbridge.com), read the company blog, and follow us on LinkedIn and Twitter.

VISIT [WWW.EVERBRIDGE.COM](http://WWW.EVERBRIDGE.COM)

CALL +1-818-230-9700

