MeriTalk
Improving the Outcomes of Government IT

ONSOLVE

A Nation on High Alert – Closing Risk Intelligence and Critical Communications Gaps

In the past year, there has been a sharp rise in civil unrest and domestic terrorism. Industry groups have warned of the growing concern and according to recent congressional testimony, the number of domestic terrorism investigations has doubled from around 1,000 in 2017 to roughly 2,000 at the start of 2021. The Department of Homeland Security (DHS) has labeled domestic violent extremism the "greatest threat" to the United States.

In the same vein, natural disasters – wildfires, flooding and widespread power outages – are becoming more common and more devastating. By December 2020 there were about 57,000 wildfires compared with 50,477 in 2019, according to the National Interagency Fire Center.

As these types of emergency situations become more prevalent and intense, there is a critical need for the Federal government to quickly detect and identify critical events, then communicate with government facilities, their staff, satellite office and other internal stakeholders about these events as they unfold.

What is Critical Event Management (CEM)?

To manage critical events, the Federal government needs three things. They first need the knowledge that something is happening – known as risk intelligence. They also need a plan for if it does happen and how they will respond – incident management. Finally, they need the ability to communicate with government facilities and their staff not only about what they should do but also about how they are responding – critical communications.

Integration of Risk Intelligence and Critical Communications

In a crisis, the most important activity is getting accurate, actionable information to the people that need it. This is not limited to the government sharing information with internal stakeholders, but also includes the government receiving information to deliver a better response. During a natural disaster, for example, the responding agency can utilize risk intelligence to identify the event and the area that will be affected and proactively contact stakeholders to not only share critical information about necessary actions, but to also receive information about necessary response.

The flow of information must be seamless – risk intelligence coming in and incident management/crisis response going out – and this requires an integrated platform.

Implementation Challenges

The Federal government is the single largest enterprise in the United States – and coordinating a cohesive solution across that enterprise is extremely difficult. Agencies need as much information as possible the moment it is available – and that information needs to be delivered directly to the people who need it. Risk intelligence is most effective when agencies are confident they will get relevant information quickly.

Take the January 6 attack on the U.S. Capitol as an example. Several agencies and departments – the Federal Bureau of Investigations (FBI), Secret Service,

U.S. Capitol Police, Washington Metropolitan Police Department and DHS – were involved that day but no agency was able to coordinate a quick response. While these agencies span different jurisdictions, having consistent insights into the situation as it was unfolding would have better positioned each agency to respond. They could better communicate with their stakeholders, share information about what areas to avoid and provide updates as they come in.

Compounding the challenge, risk intelligence is only valuable if agencies get it quickly. This requires artificial intelligence (AI) to assist internal staff, as strictly having human analysts cannot gather and process threat data quickly enough to draw conclusions and share actionable information. However, Federal agencies don't typically have a system that integrates risk intelligence and critical communications. If an agency receives actionable risk intelligence, it must be able to share that information quickly and efficiently with personnel. Agencies need an integrated platform that can detect and filter critical events then share information immediately.

The sheer size of the Federal government makes it difficult to implement a cohesive, integrated system across agencies. Each agency is responsible for its own purchasing decisions – and agencies often choose a system that works for their specific needs. For the Federal government to achieve quality CEM, it needs a scalable, flexible solution.

How OnSolve Can Help

For any one solution to work for the Federal government, it must be scalable and flexible. No matter the agency size or mission scope, the OnSolve Platform for Critical Event Management adapts agilely. By integrating risk intelligence with incident management and critical communications, agencies across the government can utilize the same platform, target specific groups and coordinate around critical events – all while working from the same risk intelligence.

Traditional risk intelligence that monitors all the internet is like looking for a needle in a field of haystacks, and it produces excessive noise. OnSolve's next-generation AI takes all of these data sources and validates them, filtering through the ones that are not credible. This enables agencies to look at the needle that is about to poke them. When agencies are confident that information is validated, they can immediately act on it. OnSolve Risk Intelligence identifies adverse events with pinpoint accuracy and calculates risks 90 percent faster than traditional one-dimensional monitoring.

When a threat presents itself, crisis response teams must be able to connect and take action. OnSolve Incident Management keeps response plans moving forward via a mobile platform that minimizes downtime, mitigates disruptions and delivers full control.

This is done with no sacrifice to security – OnSolve leverages a cloud-based Software-as-a-Service platform to deliver the reliability and scale Federal agencies require. Agencies can easily launch simultaneous alerts to personnel, residents and other key stakeholders via landlines, cellular phones, email, text, social media, mobile applications, Integrated Public Alert and Warning Systems (IPAWS), RSS feeds and more.

During a critical event, it is crucial for agencies to get relevant information to stakeholders quickly. The moment a critical event is detected, the Federal government must be able to share information with government facilities, their staff, satellite office and other internal stakeholders. Effective CEM integrates risk intelligence, critical communications and incident management – and technology today gives unprecedented power to manage critical events with speed, relevance and usability, making government facilities, their staff and ultimately, constituents, safer and more informed.