

EST  1998

DOMESTIC PREPAREDNESS JOURNAL

VOLUME 20 ISSUE 9

SEPTEMBER 2024



Remembering 9/11
Responder Appreciation

Take Domestic Preparedness



September 2024, Volume 20, Issue 9

Editor-in-Chief	Catherine L. Feinman
Editorial Associate	Christine Anderson
Project Manager	Elisa DeLeon
Publications and Outreach Specialist	Teresa Farfan
Marketing Coordinator	Nicolette Casey
Student Intern	Annette Velasco

Advisory Board

Caroline Agarabi
Raphael Barishansky
Michael Breslin
Paul Cope
Robert DesRosier Sr.
Nathan DiPillo
Kay C. Goss

Charles Guddemi
Robert C. Hutchinson
Rhonda Lawson
Joseph J. Leonard Jr.
Ann Lesperance
Anthony S. Mangeri
Sadie Martinez

Kesley Richardson
Tanya Scherr
Richard Schoeberl
Mary Schoenfeldt
Lynda Zambrano

Cover Source: Generated with Canva Free (Pro) License / DALL-E (OpenAI)

For more information about Domestic Preparedness, visit DomesticPreparedness.com

Business Office: 313 E Anderson Lane, Suite 300 Austin, Texas 78752

Copyright 2024, by the Texas Division of Emergency Management. Reproduction of any part of this publication without express written permission is strictly prohibited. Domestic Preparedness Journal is electronically delivered by the Texas Division of Emergency Management, 313 E Anderson Lane Suite 300, Austin, Texas 78752 USA; email: subscriber@domprep.com. The website, DomesticPreparedness.com, the *Domestic Preparedness Journal*, and The Weekly Brief include facts, views, opinions, and recommendations of individuals and organizations deemed of interest. The Texas Division of Emergency Management and the Texas A&M University System do not guarantee the accuracy, completeness, or timeliness of, or otherwise endorse, these views, facts, opinions or recommendations.

Source: Unsplash/Clark Young

Preparedness – The Goal With No Finish Line

By Catherine L. Feinman

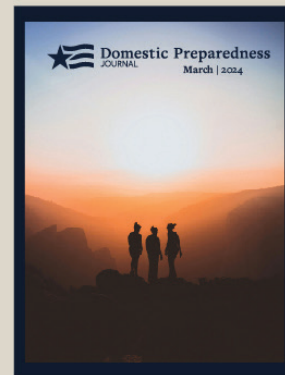
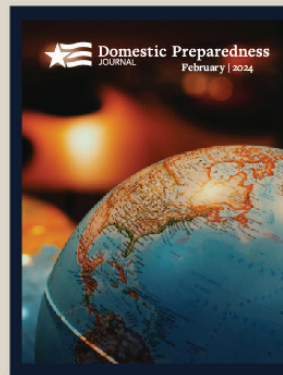
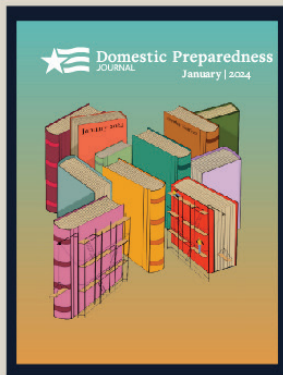
The terrorist attacks on September 11, 2001 (9/11), shocked the nation and highlighted preparedness gaps in security, communications, interagency collaboration, responder health, and other critical areas. A few years after that tragic day, the Federal Emergency Management Agency declared the month of September as National Preparedness Month to build emergency preparedness awareness and actions throughout each community.

So much has happened in the decades since 9/11. Threats have evolved, new technologies have emerged, and new partnerships have formed. There has undoubtedly been progress in the preparedness space, but there is no finish line. Community leaders must continually reevaluate their plans, procedures, and resources to adapt to changing conditions that could impact people and properties.

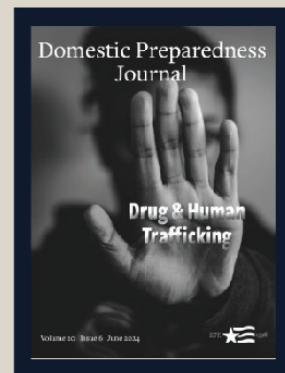
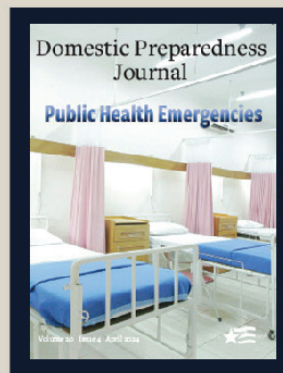
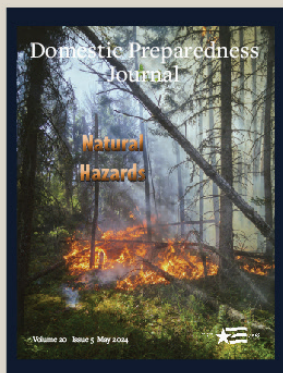
Talking to others about potential threats and hazards and what to do about them is a start. From there, these relationships can develop into valuable partnerships for sharing information and resources. Solid relationships nurture strong communities that can withstand extreme weather events, national security threats, critical infrastructure failures, and other disastrous events and can support those who tirelessly work on the frontlines.

The authors in this September edition of the *Domestic Preparedness Journal* address community outreach, responder fatigue, first responder equipment, crisis communications, and threat awareness. As National Preparedness Month approaches, national preparedness efforts cannot stop. Keep resetting goals and building capabilities and resources to help communities move toward that ever-moving finish line.

SHARE YOUR INSIGHTS



Domesticpreparedness.com/subscribe



SUBMIT AN ARTICLE TO THE JOURNAL

WWW.DOMESTICPREPAREDNESS.COM/AUTHORS

Table of Contents

Editor's Note

1 Preparedness – The Goal With No Finish Line

By Catherine L. Feinman

Feature Articles

4 National Preparedness Month 2024: Talk About It

By Ian Pleet

8 Responder Fatigue – A Growing Concern

By Dan Scherr and Tanya Scherr

14 AI and 911 Call Systems: A New Ally or a Hidden Risk?

By Michael Breslin

20 National Laboratory Partnerships: Linking Operations and Research

By Ryan Eddy and Ann Lesperance

26 Crisis Communications – Reaching Teens and Young Adults

By Barrett Cappetto

In the News

30 Thwarting Terrorist Threats at Home

By Richard Schoeberl

36 Security in and Around D.C. – Following the Informational Dots

By Catherine L. Feinman



Source: [Farknot Architect](#)/Adobe Stock

National Preparedness Month 2024: Talk About It

By Ian Pleet

Each September, the Federal Emergency Management Agency (FEMA) promotes National Preparedness Month, a campaign to educate and empower individuals and communities to prepare for emergencies. In 2024, FEMA emphasizes the importance of disaster readiness with the theme “Start a Conversation.” These campaigns are for everyone in any community, but the campaign chooses a specific focus group to highlight each year. In 2021, it was the Latino community; in 2022, it was the Black and African American community; in 2023, it was older adults; and in 2024, it is the Asian American, Native Hawaiian, and Pacific Islander (AANHPI) communities.

By focusing material in this way, these groups can better equip themselves with the necessary tools and informative resources to prepare in advance of potential disasters. In addition, these campaigns help other community members better understand the needs of people across cultures and languages. With insights from FEMA, the National Fire Protection Association (NFPA), and other organizations, this article highlights key preparedness strategies and offers actionable steps to enhance community capabilities before the next disaster.

Asian American, Native Hawaiian, and Pacific Islander Groups

On August 8, 2023, wildfires destroyed thousands of structures and claimed more than 100 lives on the island of Maui. The following after-action reports identified gaps and presented possible ways to fill them:

- The County of Maui Department of Fire and Public Safety highlighted 17 specific challenges and 111 recommendations for overcoming them. Increasing situational awareness and public involvement were among the recommendations.
- The Maui Police Department made 32 recommendations along with their progress in implementing them. Ensuring accurate public information campaigns was challenging. The department also recognized the strong community ties related to disasters:

Countless numbers of volunteers gave their time and energy at the multiple disaster shelters setup across the island. Individuals and groups donated non-perishable food items, toiletries, diapers, and clothing from their homes and even emptied the shelves of Maui’s retail, wholesale, and grocery

stores to provide items for those who lost everything in the fires.

Throughout the year, the emergency preparedness community has followed Hawaii's response and recovery efforts to find better ways to prepare these and other vulnerable populations. Then, in a May 30, 2024, press release, FEMA announced the 2024 National Preparedness theme and focus on AANHPI groups for risks and disasters. FEMA Administrator Deanne Criswell stated:

We're committed to understanding the realities of such a broad and diverse community to improve how messaging and resources reach people and help deliver our mission in a powerful, long-lasting and impactful way.

In addition, FEMA's 2023 National Household Survey exposed the following trend that creates a barrier to these communities preparing for disasters and connecting:

65% of the Asian Americans and 58% of Native Hawaiian or Pacific Islanders surveyed reported that they don't believe that taking a step to prepare will make a difference and were not confident in their ability to prepare.

With Asian Americans comprising the fastest-growing group in the United States between 2000 and 2019, FEMA's campaign underscores the necessity of readiness and encouraging communities to engage in preparedness activities: develop emergency plans, assemble disaster kits, and stay informed. Addressing any unique cultural, linguistic, and economic barriers is a critical component of preparedness for the AANHPI group's survival and recovery.

Taking Steps to Prepare

Language barriers, cultural differences, socioeconomic disparities, and other factors introduce distinct challenges for groups

like AANHPI in disaster preparedness. Such challenges can hinder effective communication, understanding of risks, and access to resources. To address these issues, FEMA has partnered with community-based organizations to develop culturally tailored outreach materials and training programs. For instance, FEMA's Ready Campaign offers multilingual resources that cater to the linguistic needs across communities. Additionally, FEMA offers train-the-trainer programs to empower community leaders to disseminate preparedness information within their networks.

The NFPA also plays a significant role in emergency preparedness by focusing on fire safety, a critical concern in many densely populated neighborhoods. NFPA's outreach efforts include fire safety education programs that are culturally relevant and accessible, ensuring that fire prevention measures are effectively communicated. Key steps that FEMA, the NFPA, and other organizations recommend for personal and family preparedness include:

- *Create a plan* – Families should discuss potential disasters and create plans that include evacuation routes, communication methods, and meeting locations. The NFPA website includes Safety Tip Sheets to assist with planning, including fire safety, escape planning, and emergency preparedness.
- *Build an emergency kit* – A well-stocked emergency kit should contain essentials such as water, non-perishable food, medications, and important documents. The NFPA also recommends including fire safety items like fire extinguishers and smoke alarms. Understanding the risks specific to one's region is crucial.
- *Stay informed* – It is imperative for community members to stay informed by monitoring local emergency alerts and signing up for community warning

systems. Recognizing that access to information in one's native language is vital, FEMA and other agencies are expanding their resources to include more languages and ensure that preparedness guidelines and resources are not only disseminated but also understood by everyone in the community.

- *Get involved* – Community organizations and leaders can play significant roles in preparedness activities. By participating in Local Emergency Planning Committees or Community Emergency Response Teams (CERT), AANHPI and other community members can contribute to their collective safety.

In observance of National Preparedness Month 2024, it is imperative that communities, including AANHPI groups, take action to protect themselves and their families. Communities can significantly enhance their ability to prepare for, respond to, and recover from disasters when all community members take steps to prepare. However, resources and information must be accessible and available to ensure no one is alone in this journey. Local leaders and community organizations play a crucial role in promoting preparedness and should collaborate with other agencies and organizations to ensure that preparedness messages reach all community members.



Ian Pleet is committed and dedicated to serving as an outstanding example of an emergency management professional with over thirty years of hands-on expertise. He is widely recognized as an adept manager of high-risk emergencies, with a strong focus on addressing chemical, biological, radiological, nuclear, and explosive threats (CBRNE), as well as weapons of mass destruction (WMD) and infectious diseases. His record of accomplishment is marked by the successful design and execution of exercises, delivering adult education using high-fidelity simulations, and establishing effective incident management systems during emergency responses. Moreover, Mr. Pleet is renowned for his ability to advocate policy and oversee program reviews, and he is considered an authority in risk management. He plays an active role in emergency

management as an instructor for emergency management and incident command courses, contributing to industry publications and providing technical oversight for textbooks before publication. He is a pro-board-certified fire officer IV, FEMA Professional Continuity Practitioner, and DoD Antiterrorism Officer.



Source: Ready.gov

Building a culture of preparedness can save lives and strengthen the fabric of society.

Preparedness is everyone's responsibility. AANHPI groups and others, with each of their unique challenges and strengths, are called upon to take proactive steps in safeguarding their future. By leveraging the resources provided by FEMA, NFPA, and other organizations, communities can overcome barriers and "Start a Conversation" that builds personal and family emergency preparedness.



E



F

C



Responder Fatigue – A Growing Concern

By Dan Scherr & Tanya Scherr

Fatigue is an educational topic for first responders such as police, fire, emergency medical services (EMS), and healthcare workers and often a constant companion in these professions. Fatigue can be defined as “a feeling of weariness, tiredness, or a lack of energy.” More than 43% of workers report being sleep-deprived, which rises to more than 60% for those working the night shift. The Brigham and Women’s Hospital Sleep Matters Initiative and the National Safety Council estimate the cost of fatigue in the workplace at \$136 billion in lost productivity. However, the cost goes well beyond the financial impact. There are also impacts on mental health, job performance, injuries, and accidents that are exacerbated by fatigue, issues that can rise in importance and affect first responders.

Manifestations of Fatigue

A 2023 meta-analysis of 43 studies on fatigue in emergency responders (paramedics, firefighters, and dispatchers) found fatigue is a prevalent issue both on- and off-duty. The study found this fatigue led to elevated depression and anxiety, along with a decrease in cognitive reaction speed. Fatigue was also commonly associated with negative outcomes for responders, including violating safety protocols, injuries, near-miss incidents, and medication errors. A previous 2017 study

notes that organizations and personnel share the responsibility for managing fatigue risks, which traditionally focused on managing the hours of service or shift length and implementing fatigue mitigation strategies. These strategies, while well-intentioned, can face a range of challenges, including buy-in, implementation, and staffing challenges, among others.

A 2022 meta-analysis including law enforcement and correctional officers found that more than half of responding officers reported poor sleep quality. Officers with a sleep disorder had a higher probability of safety violations, falling asleep at the wheel, administrative errors, negative interactions with citizens, and increased citizen complaints. With transportation incidents as a leading cause of law enforcement fatalities, the degradation of alertness and reaction speeds associated with fatigue represents a danger to officers and the public. The challenges of shift work exacerbate these risks, with officers on duty for 10 hours being 90% more likely to be involved in an accident and 110% more likely after 12 hours.

Between the demands of the job, changes in shifts, overtime, work-life balance, and the current operating environment, responders are familiar with the concept and potential impacts of traditional fatigue. Agencies

invest significant time and resources in educating personnel on the benefits of getting sufficient rest, degradation of performance, and safety considerations. It is critical, however, that agencies and leaders recognize that a lack of sleep is only one aspect of fatigue first responders deal with on any given day. Responders must also manage compassion, disaster, vigilance, and alert fatigue alongside the stresses and everyday pressures of their roles.

Compassion Fatigue – Caring Too Much

Compassion fatigue is a long-standing issue outlined by traumatology expert [Charles R. Figley](#) that describes the challenges responders face dealing with traumatic events and people in need. Even though research shows those traumatized desire a compassionate professional to assist them, that level of empathy can have an impact on the responder as well as the victim. The more engaged the responder becomes with each individual and situation, the higher the chance they share the victim's feelings, which can lead to mental and physical [exhaustion](#). To preserve themselves and meet the demands of the job, responders can become emotionally detached from events. This type of burnout is similar to disaster fatigue, where the increasing pace of major events places increasing demands on emergency management personnel, responders, and government agencies.

In the 1960s, [FEMA responded](#) to approximately 18 disasters per year. FEMA averaged 148 disasters in 2019-2023, with 315 in 2020 alone. The dramatic increase in response requirements led to burnout across the agency, which reported a [35% staffing gap](#) in 2022. This gap and ongoing agency [funding challenges](#) add pressure on the remaining staff to complete their missions with fewer

resources. The 2024 shortage of funds, which FEMA notes could reach \$7 billion by the end of this hurricane season, would be the tenth time since 2001 that the agency had to triage its response due to funding shortages. These factors, coupled with the COVID-19 pandemic, humanitarian service requests at the southern border, and extreme weather events, strain emergency managers and agencies nationwide.

Vigilance Fatigue – Information Overload

Vigilance fatigue is an issue that can impact first responders and is increasingly affecting responders in today's complex operating environment. [Vigilance fatigue](#) manifests as mistakes in identifying potential threats because of information overload, extended periods working under ambiguous threats, pressure to avoid errors, and poor or missing education on making decisions under stress. These working conditions accurately represent the basic working conditions for many first responders, particularly in the wake of the September 11, 2001, terror attacks.

Over the past 20-plus years, the threat of terror attacks, the use of social media, protests, and other persistent threats across the country have raised the stakes for every shift worked. Responders must constantly scan their environment for threats and updated information to perform their tasks safely and efficiently. Like the others described, this type of fatigue is exacerbated by lack of sleep, further complicating addressing the issue. Available [resources and feedback](#) on the effectiveness of efforts and awareness also impact continued vigilance. If personnel believe they are making the best decisions and already know some vectors are safe or how a situation will play out, they may get complacent or stop fully evaluating threats.



Domestic Preparedness
JOURNAL

Subscribe today.



Scan the QR code or
visit the link below

www.domesticpreparedness.com/subscribe

Alert Fatigue – Desensitization

Alert or alarm fatigue is also a persistent and growing problem for responders. Alert fatigue occurs when the number of alerts or alarms [desensitizes](#) an individual responsible for response, leading to delays or ignored events. This type of fatigue takes different forms but is an area of concern in healthcare, cybersecurity, emergency management, and traditional first responder roles. The pressures and concerns noted in the previous sections outline some of the limitations and challenges responders manage in their daily work. These may exacerbate the alert fatigue issue as responders strive to maximize the use of resources and effectiveness to meet increased service demands, budget limitations, and staffing shortages.

For cybersecurity responders working to secure businesses, agencies, and critical infrastructure, alert fatigue is also a persistent threat. On average, [security operations center](#) teams see 4,484 alerts daily, and two-thirds of those alerts are ignored. The same report noted that 97% of respondents were concerned they have or will miss a security threat buried among the noise of routine alerts. Analysts also reported that 83% of the alerts they received were false positives, reinforcing the disconnect between the alerts and the severity of the threats. The manual triage performed in most security operations centers costs over \$3 billion annually in the United States.

[Research](#) in healthcare shows that 72-99% of clinical alarms are false. With such a preponderance of false alarms, the systems in place train clinical staff that the audible warnings are not an immediate threat or are most likely not important. This desensitization was on display in a 2013 [case](#), where a pediatric patient at the

University of California, San Francisco Medical Center (consistently one of the top ten hospitals in the United States) was administered almost 39 times the required dose of an antibiotic and suffered a grand mal seizure. The resident ordered the medication for the patient through a series of steps, entered the wrong conversion into the system, and then ignored the alert message on the screen. An investigation into the incident revealed that hospital pharmacists received alerts on nearly 175,000 orders per month, and about half entered the system. The burden on physicians was significantly less, but doctors still received [17,000](#) monthly alerts. Like the constant audible alerts in the clinical space, the continuous stream of pop-ups desensitizes users to potential dangers, particularly when alerts are overridden based on proper procedures and medical needs.

An investigation by the [Boston Globe](#) in 2011 found more than 200 deaths in 2006-2011 were attributed to issues with patient alarms. A [Clinical Alarms Summit](#) in 2011 also addressed this phenomenon and published ten actions to take immediately and a plan to prevent alarm fatigue-related deaths by 2017. The American Association of Critical Care Nurses then published best practices in 2013, with updated protocols in 2018. A [review in 2020](#) of intensive care unit nurses found that 95% of respondents felt the burden of alarms, and 93% thought excessive alarms could be ignored or muted, mainly due to repeated false alarms.

Combating Worker Fatigue

An evaluation of alerts is a priority. Reviewing the [thresholds](#) of alerts can provide insight into the current operating environment and reveal potential changes:

- Are alerts set too high or low?
- Do alerts need to be addressed immediately when the alarm sounds?
- Is there another method to provide notice if the alarm is informative or not an immediate concern?

As noted in the previous overdose example, all alerts in that system were provided in the same manner. Providing a variety of alarm types, based on preferred factors for the organization, could better engage with the responder. Consolidating “like” alerts and ensuring the alerts signify an actionable event to correct the deficient area can increase engagement and reduce wasted energy and effort.

In the [technical environment](#), organizations can assist personnel by using automation to detect common threats and take corrective action when appropriate. By leveraging technology to correct these low-stakes, routine issues, security personnel can focus on concerns that need their attention while avoiding repetitive alarms and mundane corrections.

Evaluating the safety and operations of first response agencies requires consideration of not only standard metrics and traditional concerns like sufficient sleep but also complications that can impact personnel’s mental health and awareness. The concepts of fatigue discussed here are not new, but factors in today’s operating environment complicate them. The increasing rate of disasters, limited resources, and continuous access to information streams can be overwhelming to citizens, but much more so for those responding to emergencies. The *constant on* society with endless notifications at work and home forces people to choose which *important* messages to read, engage with, or ignore. This fatigue and behavior can follow into the workplace. Reviewing policies and procedures and helping emergency responders manage that workload with alerts triaged for importance and immediacy can reduce fatigue and improve overall outcomes.



Dan Scherr holds a Ph.D. in Public Policy Administration with a terrorism, mediation, and peace focus. He is an assistant professor in Criminal Justice and Homeland Security at the University of Tennessee Southern and program coordinator for the Cybersecurity Program. He is also a co-director of the Honors Program. He is a Certified Fraud Examiner and Army veteran who served stateside during the September 11th attacks and has over two decades of experience in homeland security and operations.



Tanya Scherr holds a Ph.D. in Public Policy Administration with a healthcare and emergency preparedness focus. She is an associate professor in Healthcare Administration for the University of Arizona and has three decades of healthcare experience. Along with being a Certified Fraud Examiner since 2011, she is also a former firefighter-emergency medical technician (EMT), previously licensed in several states, and held national certification. She has held several executive and board of director positions for community nonprofits that focus on women’s equality, domestic violence, and sexual assault.



Source: [Олександр Луценко](#)/Adobe Stock

AI and 911 Call Systems: A New Ally or a Hidden Risk?

By Michael Breslin

In today's world, where the unexpected can strike at any moment, the systems designed to protect people – 911 call centers – are facing unprecedented challenges. From natural disasters to sophisticated cyberthreats, the risks to public safety are evolving fast. For example, a devastating [wildfire in Lahaina, Maui](#), in August 2023 destroyed much of the town, causing significant loss of life and property. The call volume overwhelmed [911 dispatchers](#). A ransomware attack on [Change Healthcare](#) in February 2024 caused massive disruptions in the U.S., including [outages](#) with some 911 call centers. Yet, these critical lifelines are often hampered by outdated technology, limited resources, and the delicate balance between ensuring security and preserving personal freedoms. Behind each call for help is a human life at stake. As these threats grow more complex, so too does the responsibility of those tasked with responding. The current environment is a delicate and dynamic one, where the consequences of failure can be devastating, whether from human error or the limits of precautionary measures.

The [Principles of Communication](#) are vital during routine and emergency situations

involving the reporting and assessment of an event to the dispatch and the utilization and response of law enforcement and public safety professionals. The most effective use of resources for appropriate response and risk mitigation can be hindered by poor communication among and between the public and first responders. Unfortunately, the challenges of poor interoperability and means of communication among law enforcement and public safety professionals continue to be [a national problem](#), with over two decades of intermittent progress, incomplete measures, and sporadic attention. Additionally, the complexity and uncertainty that are characteristic of crisis situations add to the [“fog of war”](#) and may also delay, impede, or otherwise negatively impact the communication inherent in successful public safety efforts.

And Now Artificial Intelligence (AI)...

One facet of homeland security and public safety subject to increased efficiencies and risks associated with advancements in technology is the nation's 911 call systems. These systems play a pivotal role in ensuring swift and effective

emergency responses. The integration of AI technologies can significantly enhance these systems. AI and its impact on critical domains are crucial to homeland security. The public relies on the 911 call system during emergencies and crises.

It is not a far stretch to imagine the deafening sounds of a fire truck racing to a three-alarm fire, the arrival of a police squad car at the scene of an assault, or the swift departure of an ambulance carrying a heart attack victim to the nearest emergency room. These scenarios are initiated and depend on a reliable and trustworthy 911 call system. These three numbers (911) and subsequent emergency response can be the difference between life and death.

However, this lifeline is plagued with problems due to antiquated systems, funding shortfalls, and inadequate staffing, training, and capabilities. [Shortcomings](#) of the 911 call system cause service delays and outages. These failures occur across the country and add to the challenges of public safety and preparedness.

The Pros and Cons of AI for First Responders and 911 Systems

The integration of AI technologies can significantly enhance these systems and benefit society. Some pros and cons of using AI for first responders and 911 emergency call systems, along with examples of the challenges and benefits, are listed below.

Pros:

1. *Faster Response Times* – AI can process information rapidly, [helping dispatchers prioritize](#) urgent calls and allocate resources efficiently. *Example:* Real-time

location tracking and video capabilities assist responders in reaching emergency scenes faster.

2. *Automated Call Routing, Triage, and*

Decision Support – AI algorithms can intelligently route emergency calls to the nearest dispatch center based on location data. This reduces response time and ensures that help reaches the scene promptly. AI algorithms can assess the severity of calls and provide recommendations to dispatchers. *Example:* AI-based tools help identify life-threatening situations and guide responders accordingly.

3. *Natural Language Processing (NLP) and Language Translation* – AI-powered NLP models can transcribe and analyze callers’ speech, extracting critical information even when the caller is distressed or unable to communicate clearly. AI can instantly translate calls in different languages, bridging communication gaps. *Example:* A dispatcher can communicate effectively with non-English-speaking callers.
4. *Predictive Analytics* – AI analyzes historical data to predict emergency trends, allocate resources proactively, and optimize emergency services’ deployment. *Example:* Predictive models

The reality is the system of 911 as it is today across the country is still kind of operated off technology that was developed in the 1930s.
– Ty Wooten, director of government affairs for the International Academies of Emergency Dispatch
[AI bots are helping 911 dispatchers with their workload • Stateline](#)

anticipate spikes in call volume during natural disasters.

Innovation in AI technologies and the increased efficiencies that follow are not risk-free. There are potential [barriers](#), concerns, and considerations.

Cons:

1. *Bias and Fairness* – AI systems may inherit biases from training data, affecting decision-making. AI systems must be trained on datasets to avoid biases related to race, gender, or socioeconomic status. Biased algorithms could inadvertently impact emergency response decisions. *Example:* An AI algorithm might inadvertently prioritize certain neighborhoods over others.
2. *Privacy Concerns* – Balancing the need for efficient emergency services with privacy rights is crucial. AI processes sensitive information during calls, raising privacy issues. The systems should handle sensitive information securely to protect the public and promote trust. *Example:* Balancing data collection for emergency response with privacy rights.
3. *Overreliance and Errors* – Relying solely on AI can lead to mistakes or missed critical details. *Example:* An AI system may misinterpret a caller's distress level due to speech nuances.
4. *Human Interaction and Empathy* – AI lacks human empathy and emotional understanding. *Example:* Callers may need emotional support during distressing situations.
5. *Trust and Transparency* – Community members may be skeptical of AI-driven responses. *Example:* Use of AI could lead to further mistrust in law enforcement and public safety agencies

These are samples of the benefits and challenges for the community posed using AI-driven 911 systems. Striking the right balance between AI assistance, data-driven decision-making and human judgment is crucial. Overreliance on AI could impact critical decision-making. [AI offers significant advantages](#) for managing call volumes and emergency response and improving efficiency. However, careful implementation and ongoing evaluation are essential to maximize benefits while addressing potential drawbacks.

Although few states (e.g., Colorado, Maryland, Missouri, Oregon, South Carolina, Texas, and Virginia) have established clear [AI regulatory frameworks](#) for emergency call centers, some progress has been made in addressing the vulnerabilities of an AI-infused call system. For example, some actions and regulations undertaken by public safety agencies and police professionals aim to protect communities from the malicious use of AI in emergency dispatch services.

The identification and disruption of malicious AI actors is vital. Organizations like [OpenAI](#) collaborate with partners to detect and disrupt state-affiliated threat actors using AI for cyberattacks. Mitigation efforts include terminating accounts associated with malicious actors, which helps prevent misuse of AI services. Prescribed guidelines for AI bots in 911 centers are essential for balancing efficiency and accuracy in AI use while addressing bias concerns and potential errors in AI responses.


Emergency Services as a Likely Target for Cyberattacks, Warns DHS

Despite no widespread reports of 911 call systems being directly hijacked by malicious AI, concerns about the potential risks exist. Akin to the nation's critical infrastructure, the nation's 911 emergency services and

call systems are also potential targets and vulnerable to exploitation and cyberattacks. Following is a hypothetical scenario and possible mitigation steps to explore.

Scenario: AI-Driven 911 System Hijacking

- *The Setup* – A mid-sized city with an AI-enhanced 911 system relies on machine learning algorithms to process emergency calls. The AI system is trained to recognize distress signals, prioritize calls, and dispatch appropriate responders.



CALLING 911 IS MEANT TO SAVE LIVES.
BUT THE EMERGENCY SERVICE, AND
OTHERS LIKE IT, ARE ALSO VIEWED AS
RIPE TARGETS FOR CRIMINALLY MINDED
CYBER-ATTACKERS,

<https://abcnews.go.com/US/emergency-services-target-cyberattacks-warns-dhs/story?id=109348647>

- *The Attack* – Malicious actors exploit vulnerabilities in the AI system:
 - *Adversarial Inputs* – They craft fake emergency calls designed to confuse the AI.
 - *Data Poisoning* – They manipulate training data to bias the AI's decision-making.
 - *Model Tampering* – They compromise the AI model itself.
- *Consequences*:
 - *False Prioritization* – The AI misclassifies critical calls, leading to delayed responses for life-threatening emergencies.
 - *Resource Misallocation* – Responders are dispatched to

non-emergencies, leaving genuine emergencies unattended.

- *Chaos and Panic* – The public loses trust in the 911 system, causing panic during real crises.
- *Attack Examples*:
 - *Swatting Attacks* – Malicious actors use AI-generated calls to falsely report emergencies (e.g., bomb threats, active shooters) at specific locations. Responders rush to the scene, wasting resources.
 - *Data Poisoning* – By subtly altering training data, attackers bias the AI to ignore certain types of calls (e.g., domestic violence) or prioritize others (e.g., high-profile areas).
- *Mitigation*:
 - *Robust Testing* – Regularly test the AI system against adversarial inputs.
 - *Human Oversight* – Maintain human dispatchers alongside AI to catch anomalies.
 - *Secure Training Data* – Prevent data poisoning by carefully curating training datasets.

This hypothetical scenario is not much different than the potential reality faced by the law enforcement and first responder profession and the public. The challenges for improving operability have been outlined and, like others facing homeland security professionals, the need for additional funding is common. The annual spending on 911 call systems varies by state and locality.

National View: 911 Data

In 2015, 40 states and the District of Columbia collectively spent approximately \$3.4 billion on 911 services. The National 911 Annual Report and the National 911 Profile

Database provide more recent and specific data, including an interactive version of the most recent data.

The National 911 Annual Report is a collaborative effort between the National 911 Program and the National Association of State 911 Administrators (NASNA). Each year, they collect comprehensive data related to 911 services, including funding, revenue, text-to-911 implementation, and progress toward Next Generation 911 (NG911). This data is voluntarily submitted by states and compiled in the National 911 Profile Database.

The report analyzes trends and provides segmented information for state 911 leaders, legislators, and policymakers to make informed decisions about emergency services. The latest report covers [2021 data](#), and previous reports are available for reference. The [Profile Database](#) captures details about a state's 911 operations, protocols, and progress, helping enhance emergency response nationwide.

The [2021 National 911 Annual Report](#) revealed several noteworthy findings across statewide plans. Thirty-three states reported having a statewide Next Generation 911 (NG911)

plan. NG911 aims to enhance emergency communication infrastructure and services along with adoption of the Emergency Services IP Network ([NG911 ESInet](#)). Over 2,000 Public Safety Answering Points (PSAPs) across 46 states reported using an Emergency Services IP Network (ESInet). ESInets facilitate efficient call routing and data exchange in emergencies. Also, in 38 states, nearly 600,000 texts-to-911 were received during the calendar year. The Text-to-911 feature provides an alternative communication channel for those unable to make voice calls.

In summary, artificial intelligence is a double-edged sword in the realm of public safety and security. On one side, it empowers emergency responders, fortifies defenses, and enhances the ability to predict and respond to crises. On the other, it carries risks that, if not carefully managed, could compromise the systems it seeks to strengthen. To fully harness the power of AI while protecting society, community stakeholders must ensure its responsible implementation, prioritize transparency, and uphold rigorous ethical standards. The balance between innovation and caution will determine whether AI serves as a community's greatest ally or a hidden danger in the shared mission to protect human lives.



Michael Breslin is a retired federal law enforcement senior executive with 24 years of law enforcement and homeland security experience. He served as the deputy assistant director in the Office of Investigations focusing on the integrated mission of investigations and protection with oversight of 162 domestic and foreign field offices. He served as the event coordinator for the National Special Security Event Papal visit to Philadelphia in September 2015 and was appointed by the Secretary of Homeland Security to serve as the federal coordinator for the Papal Visit to the Mexico-U.S. Border in 2016. He is a member of the Senior Executive Service and is a published author of numerous articles on homeland security, defense, and threat mitigation methods. He serves on the Cyber Investigations Advisory Board of the U.S. Secret Service and is a Board Member for the

National Center for Missing and Exploited Children. He also serves on the Preparedness Leadership Council. He has a B.A. from Saint John's University, Queens, NY, an M.S. in National Security Strategy and a Graduate Certificate in Business Transformation and Decision Making from The Industrial College of the Armed Forces; and an MPA from John Jay College of Criminal Justice.



Source: AI-generated by [sommersby](#)/Adobe Stock

National Laboratory Partnerships: Linking Operations and Research

By Ryan Eddy and Ann Lesperance

In 2001, the September 11 (9/11) terrorist attacks spurred a pivotal change in the way the U.S. looks at preparedness for threats to the homeland. The two-plus decades that followed have been filled with collaborations, innovations, and partnerships that transformed the nation's preparedness and response capabilities. At Department of Energy national laboratories, researchers are tackling complex problems through innovative science and technology, supporting national security through research and development (R&D). Science and technology partnerships with national laboratories are helping to bridge the gap between R&D and emergency preparedness needs in the field. Pacific Northwest National Laboratory (PNNL) has developed a novel model of preparedness to link first responders, emergency managers, and critical infrastructure providers to researchers.

Understanding the Evolving Threat Landscape

With the collision of emerging technologies and increasing natural and human-made threats, the preparedness landscape is changing, and it is changing *fast*. In the 21st century, preparedness is multi-domain, multi-hazard, and multi-discipline as threats grow increasingly complex, whether digital, physical, or airborne. For emergency managers and first responders tasked with keeping communities and critical infrastructure safe, the pressure is

on to rapidly assess incoming information and make decisions faster than ever.

For more than a decade, teams at PNNL have been connecting with first responders and emergency managers across the nation to elicit feedback about technology needs in the field. Through workshops, interviews, focus groups, roundtables, and simple conversations, they have heard directly from fire, law enforcement, emergency medical services (EMS), public safety communications, critical infrastructure owners and operators, and more. In recent years, particularly with the proliferation of artificial intelligence (AI), soft-target attacks, and cascading impacts from cybersecurity breaches on critical infrastructure, each frontier poses new technological challenges and opportunities. Here are a few examples:

- **Cybersecurity.** As systems become increasingly digitized and connected, the threat surface expands. Small municipalities and their critical infrastructure owners and operators can lack the capital and resources to employ robust cybersecurity capabilities to protect themselves and the communities they serve. Preparedness demands accessible, affordable solutions to identify and elevate threats and vulnerabilities, enhance resilience through advance planning, and strengthen the security and reliability of infrastructure and cyberspace.

- *Integration and interoperability.* While new technology – such as whizbang sensors, audiovisual capabilities, and wearables – comes to market at a record pace, adoption is often fraught with delays because the jurisdictions that need it do not have the time to test, evaluate, and implement it within existing systems and data architectures. The challenge escalates with cross-jurisdictional information sharing and the privacy and policy implications that accompany it.
- *Communications.* In some spaces, there is more power in mobile devices than some first responders can use in the field. The handheld radio remains the trustworthy standby where network conditions and audio capabilities cannot keep up with the places first responders go.
- *Geolocation.* The combination of geolocation and haptic alerts (vibrations) in today's mapping tools could alert responders in low-visibility and low-audio scenarios (e.g., notify firefighters entering a danger zone or send updates to law enforcement navigating an active shooter scenario).
- *Resource Management.* Preparedness and response require many resources (people, personal protective equipment [PPE], vehicles, volunteers, etc.) that require a lot of effort, energy, and capabilities to identify and track. Imagine a system that could source PPE supplies, identify needed hospital capacity for patient transport, or quickly distinguish credentials and deploy volunteers arriving on scene.
- *Soft-Target Protection.* From sports arenas and concert venues to busy city centers, large venues are packed with people. Well-populated and unprotected places present complex security challenges that make them vulnerable to attack. Tools like systems of sensors connected with immersive visual and data analytics can reduce that threat and increase security, all while being minimally intrusive or disruptive to the carefree experience people are seeking.
- *Threat and Hazard Detection.* Chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) threats are becoming more sophisticated and making it more difficult to prepare equipment and to detect potential threats. For example, the chemical structure of fentanyl is constantly changing and difficult for detection equipment manufacturers to keep pace. Solutions are needed to discover novel signatures of emerging CBRNE threats, to update the equipment used to detect them, and to train responders in their use.
- *Critical Infrastructure.* The nation's complex and intricate systems – the electrical power grid, transportation systems, banking and finance systems, and more – is becoming more complex, more connected, and more vulnerable to adverse conditions, such as cyber and physical attacks. Modeling, simulation, and predictive analytics provide a better understanding of the system and asset interdependencies and anticipate how their disruption could impact continuity of operations in public health and national security.
- *Artificial Intelligence (AI).* The emerging and escalating capabilities of AI, including generative AI, machine learning, and automation, pose promise and peril to the future of preparedness. Even baby steps – like generative AI for public messaging, translation, or scenario planning – require a better understanding of and training with AI tools, in addition to controlled test-bed environments, standard operating procedures, and governance to ensure safe and secure operations.

Partnering for Preparedness

Recognizing that partnerships for preparedness happen in all shapes and sizes, PNNL has put connecting with end users and making regular

and consistent contact with first responders and emergency managers at the forefront of R&D outreach. This spurred the launch of the [Northwest Regional Technology Center](#), a one-of-a-kind center focused on building relationships for regional preparedness, response, and recovery. These partnerships help build informed, functional solutions that fit the emerging needs of first responders and others on the front lines. For example, teams are [reimagining the traveler experience](#) and [developing and deploying technologies to protect airline passengers](#). Some tools help protect crowded places, and others leverage capabilities like AI, satellite imagery, and predictive analytics to improve situational awareness of and response to natural disasters like wildfires and floods. Researchers are also in the fight against fentanyl, [updating chemical libraries, evaluating equipment, and informing standards](#) to improve detection equipment used by first responders in the field.

Through a [mix of projects and partnerships](#) to connect with first responders and emergency management stakeholders, PNNL is assessing current research in emergency management, eliciting and refining capability needs from

practitioners, and identifying where technology such as AI may benefit the future of emergency management and operations centers. Whatever challenges lay ahead, end-user input and an in-depth understanding of the R&D and technology landscape will help inform solutions for preparedness for years to come.

PNNL is not alone in this mission – Department of Energy national laboratories across the country are at work on all these fronts. As federally funded R&D centers, national laboratories are a conduit for connecting science and technology with the nation’s capacity to anticipate and mitigate threats. In particular, the Homeland Security Act of 2002 authorized the Department of Homeland Security to use national laboratories in conducting its mission. Having a national laboratory nearby means streamlined access to R&D talent and science and technology capabilities, including test beds, facilities, and real-time disaster support (modeling, simulation, etc.). Together, this network of talent, innovation, and partnerships can bring a science and engineering approach to preparedness and play a role in nearly every layer of the country’s national security.



[Ryan Eddy](#) serves as the director for Homeland Security Programs in the National Security Directorate at PNNL. He oversees the work PNNL performs for the U.S. Department of Homeland Security (DHS), which encompasses nearly 50 diverse projects and over \$100 million worth of annual business. Eddy manages a team that engages with components across DHS in such areas as explosives detection, nuclear security, and cybersecurity. By drawing on his years of experience in Washington, D.C., Mr. Eddy oversees program development strategies for DHS sponsors that assure PNNL is delivering mission-relevant work. DHS sponsors at PNNL include the Countering Weapons of Mass Destruction Office, Science & Technology Directorate, Customs and Border Protection, the Cybersecurity and Infrastructure Security Agency, Transportation Security Administration, and others.



[Ann Lesperance](#) is the director of the [Northwest Regional Technology Center](#) at PNNL. She has over 30 years of experience as a researcher and project manager, and her primary focus is developing regional programs to accelerate the demonstration and deployment of new homeland security technologies. Lesperance works with state and local emergency responders and public safety officials and builds regional coalitions of emergency management professionals to understand and help prioritize their operational needs and requirements. Ms. Lesperance also has a joint appointment as the director for the College of Social Science and Humanities Programs at Northeastern University Seattle. In this role, she leads efforts to build the master’s program in Security and Resilience Studies and Urban Informatics. She was also awarded a faculty affiliate appointment with Northeastern’s Global Resilience Institute, where she partners with the institute to identify and participate in interdisciplinary proposal efforts for new research and education collaborations.

A hand holding a smartphone is the central focus, with a vibrant purple and blue background. Numerous white and blue digital icons are scattered around the phone, including musical notes, speech bubbles, envelopes, a calendar, a laptop, a camera, and a person icon with a plus sign. The overall aesthetic is modern and tech-oriented.

GENERATION Z

Crisis Communications – Reaching Teens and Young Adults

By Barrett Cappetto

Crisis communication, simply put, is the theory and application of how organizations share critical information about emergent situations. Much like how emergency management is a cycle, crisis communication is cyclical and should include communication before, during, and after an event. While all phases of the cycle are essential components of any organization's public relations and crisis management plans, public alerts and warnings are the most critical for the preservation of life and property. Public safety professionals responsible for sending these notifications bear a heavy burden of balancing public welfare and their organizations' reputations.

Generational Communication Considerations

A quick internet search of emergency alerts yields a host of public warning gaffes, such as [the 2018 Hawaii ballistic missile threat](#) or biopic stories of individuals who [failed to evacuate disaster zones due to not receiving a timely alert](#). When agencies fail to deliver concise, clear, and timely emergency information, it often draws public ridicule and less-than-desirable press coverage.

Generational differences show up in unique and unexpected ways every day. The distinction between these cohorts is apparent in environments such as the workplace, the classroom, and within family units. From preferences in communication methods, tastes in music, ideas on family and marriage, and attitudes toward work and education, there is polarity between these groups. Technology, media, and entertainment have kept current with the evolving trends and preferences of the younger generation. Public safety practitioners should emphasize the same level of focus on staying agile and adapting to changing preferences and trends.

Generation Z and younger millennials' reception of crisis communication is unique from other generations because, as of now, the most significant world event they have experienced and remember was the COVID-19 pandemic. The fallout of the virus [scarred many of their peers](#) as their generation had fewer face-to-face contacts than those in other generations and reported the highest rates of depression.

There was a *whiplash* effect in the virus's infancy as public health officials and emergency managers attempted to

understand how to best respond. In addition to massive amounts of misinformation through social media, young people were confused and began to question what the pandemic meant for [their future](#). Many coming-of-age celebrations, such as graduations, the first-year college experience, high school senior year, and milestone birthdays, were canceled or significantly different than how they imagined. As a result, there was a surge of young people [self-reporting symptoms](#) of clinical depression, anxiety, and loneliness.

Breaking Through Generational Barriers

Generalizations are not accurate for everyone within any generation. However, studies reveal common characteristics that can assist agencies and organizations in developing more effective crisis communications plans for the entire community. Four action items that would help ensure public safety alerts and warnings reach younger generations are establish trust before the first alert, keep it simple, provide updates, and cast a wide net.

1. Establish Trust Before the First Alert

Generation Z's implicit [trust in institutions](#) such as the government, the criminal justice system, and the media has dwindled compared to their older counterparts. Organizations should establish relationships with their audience, conveying open and honest dialogue regarding emergency preparedness, incident response, and recovery. The audience needs to genuinely believe that, in an emergency, the information these institutions transmit is intended to keep them safe, not just “checking a box” or meeting a regulatory requirement.

2. Keep It Simple

Information conveyed in an emergent situation needs to be readily received and understood. Emergency communication should indicate who is sending the alert, what the public is expected to do, where the hazard is, and how long the condition might last. The Federal Emergency Management Agency (FEMA) has created a tool to help public safety professionals craft these [templates](#) and have them ready before an incident occurs. Although FEMA designed this resource for Integrated Public Alert and Warning System (IPAWS) users, it is useful for any dissemination platform.

3. Provide Updates

Emergency managers should prioritize sending updated information as necessary – for example, giving the “all-clear” once the situation has been resolved or when issuing guidance and updates related to the event. In the event of a lockdown due to an active assailant threat, public safety personnel should continue advising a secure-in-place and guidance to keep clear of specific areas.

One stereotype about Generation Z and millennials is they are impatient and crave instant gratification. That is a big generalization, but the younger generation does expect information to flow in real time as it becomes available. Younger generations can become frustrated with extended wait times for information or assistance, which may escalate during a stressful situation such as a natural disaster or secure-in-place event.

4. Cast a Wide Net

When sending public alerts, consider multiple avenues for notifying the audience. Younger community members may be more apt to read a text message, while older people may feel more comfortable with a phone call.

Regarding Generation Z and millennials, 59% of respondents in an August 2024 [Robert Walters survey](#) stated they preferred instant messaging and email over phone calls. Some younger audiences may ignore a phone call, especially if it comes from a phone number they do not recognize.

Also, just because a segment of the community is younger does not necessarily translate to digital literacy. Surprisingly, the “digital native” generation is among the least computer-literate groups today. According to a study published by [Dell Technologies](#) in December 2022, 44% of young people surveyed felt they acquired only basic computer literacy skills, and 12% reported they received no formal education on digital skills. Low-tech options such as sirens, public address systems, and door-to-door notifications provide a last-resort safety net to reach people of any generation, whether or not they have access to electronic devices. An emphasis on inclusivity should be made when selecting notifications to account for those with visual or hearing impairments. Additionally, care should be taken to account for community members who may lack English language proficiency.

Managing the Future of Mass Messaging

Few areas of emergency management and public safety have evolved as much as public alert and warning technology within the



Source: [PX Media](#)/Adobe Stock

past few years. From the advent of IPAWS and the first Wireless Emergency Alert (WEA) in 2012 to the broad implementation of changeable message signs and the adoption of mass messaging software, the future of public alerts and warnings is becoming increasingly more advanced. While much focus has been on the technology infrastructure, it is increasingly important to focus on the methods, practices, and theories behind handling crisis communications.



Barrett Cappetto is a pipeline controller with Colonial Pipeline Company. He is responsible for coordinating control center security and operational readiness. Previously, he served in emergency management and law enforcement roles within the University System of Georgia institutions. He is a graduate of Georgia Highlands College's Bachelor of Science in Criminal Justice and is an alumnus of the Federal Emergency Management Agency's Emergency Management Basic Academy.



COMBAT TERRORISM COMBAT TERRORISM

Source: [Sean K/Adobe Stock](#)

Thwarting Terrorist Threats at Home

By Richard Schoeberl

September 11, 2001 (9/11), with the tragic loss of nearly 3,000 lives, was the worst attack on American soil since the Japanese attacked Pearl Harbor in 1941. That day set in motion major changes to counterterrorism policies and practices, as well as changes throughout the intelligence community. Those events propelled the U.S. into two major wars and led to the establishment of the U.S. Department of Homeland Security (DHS) and the implementation of extensive surveillance measures nationwide. Undoubtedly, 9/11 permanently altered daily routines. In many ways, it also reshaped how people think of conflict, personal safety, and the safety of others.

Although the U.S. has not experienced a similar scale attack since, policymakers and national security experts debate the probability of such a tragedy happening again on U.S. soil. More than two decades later, many Americans question, “Are we any safer?” particularly with events as recent as September 2024 when a “would-be” terrorist was [arrested](#) in Canada and accused of planning a mass shooting at a Jewish center in New York City in support of the Islamic State terror organization. The scale was aspirational, but the ongoing heightened threat to national security remains.

Terrorist Threats Across Decades

Four years before al-Qa’ida operatives attacked the World Trade Center and the Pentagon in 2001, then-Central Intelligence Agency (CIA)

Director George Tenet [testified](#) publicly several times about the existential threat al-Qa’ida posed to U.S. interests domestically and abroad. Tenet [said](#), “the system was blinking red.” According to the [9/11 Commission](#), at the beginning of 2001, officials were receiving frequent reports about threats that appeared to be emerging from almost everywhere the U.S. had interests. Despite those intelligence concerns, Americans view terrorism as a less critical threat than they did following the 9/11 attacks. According to [research](#), in 2002, roughly 9 out of 10 Americans viewed terrorism as a critical threat versus only 6 out of 10 Americans in 2022. Americans’ concern about international terrorism has declined considerably in recent years.

Fast-forward decades later, Federal Bureau of Investigation (FBI) Director Christopher Wray [testified](#) before Congress that the terrorism environment is quite “elevated” and further “heightened” following the Hamas attack on Israel on October 7, 2023. The [FBI](#) believes that the danger of an Islamic extremist-inspired terrorist attack inside the U.S. is at the highest point since 9/11. Director Wray, [testifying](#) at the annual “Worldwide Threats” congressional hearings in March 2024, stated that:

Even before the October 7th attacks, I would have told this committee that we were at a heightened threat level from a terrorism perspective – in the sense that it’s the first time I’ve seen in a long,

long time, the threats from homegrown violent extremists that is jihadist-inspired extremists, domestic violent extremists, foreign terrorist organizations, and state-sponsored terrorist organizations all being elevated at one time since October 7, though, that threat has gone to a whole other level. And so, this is a time I think for much greater vigilance, maybe been called upon us.

One area of current major concern is the ongoing threat of the homegrown violent extremist in the U.S. Although not “official” members of terror organizations, these individuals are typically the lone actors who merely draw inspiration from the actions of both domestic and foreign terrorist movements. In Director Wray’s [testimony](#) before the Judiciary Committee in December 2023, he stressed that the greatest threat to the U.S. stemmed from homegrown violent extremists, citing that the homegrown violent extremist “is the greatest, most immediate international terrorism threat to the homeland.”

The October 2023 Hamas attack and Israel’s military response have increased tensions regionally and abroad, particularly with the continued media coverage of the destruction in Gaza and the loss of life that localized social media campaigns amplify. In turn, new narratives are created in neighboring countries and beyond. Israel’s military response in Gaza and Lebanon coupled with the support from the U.S. could generate a breeding ground for the next generation of terrorists. Israel says it wants to [destroy Hamas](#) and its supporters like Hezbollah, but military operations alone (like those Israel has implemented in Gaza and Lebanon) cannot prevent radicalization. In retrospect, the world witnessed this with the [creation](#) of another terror movement following the 2003 U.S.-led invasion of Iraq, which ultimately produced the Islamic State terror organization.

In 1997, the [U.S. State Department](#) listed [Hamas](#) as a designated terrorist organization that seeks to destroy Israel but has also been historically rooted in international political Islam and participated in elections, resulting in strong global influence in the Islamic community. The collateral damage created from the Gaza conflict could likely become the best recruitment tool for Hamas or far worse, from another terror group the world has not yet seen. The current projections will increase the risk to Israel and the U.S. through mass radicalization. As with prior conflicts in the Middle East, the recent fighting in Gaza and Lebanon will likely trigger terrorist consequences elsewhere in the region. At the annual hearing on global security threats, Director of National Intelligence [Avril Haines](#) stated, “The crisis [in Gaza] has galvanized violence by a range of actors around the world. And while it is too early to tell, it is likely that the Gaza conflict will have a generational impact on terrorism.”

Mass Radicalization Efforts

The explosion of social media presents an extraordinary view into mass radicalization. Social media makes it possible for a story [good or bad] to spread in real time. People are now interacting on platforms without knowing one another personally. However, these virtual communities with extremist messaging or created narratives can promote and foster a mobilization of hundreds or thousands of individuals under a common ideology, an injustice, or a grievance. The underlying political message of the idealist battle is apparent in the following examples:

- The number of [attacks](#) on U.S. military bases overseas by Iran-backed militia groups have risen;
- Cyberattacks against the U.S. by [Iran](#) and non-state actors have risen; and

- There are ongoing plots against the U.S., including the [Canadian](#) who attempted to enter the U.S. to carry out a mass shooting at a Jewish Center in New York City.

According to FBI Director Wray, “since October 7, we’re working around the clock to identify and disrupt potential attacks by those inspired by Hamas’s horrific terrorist attacks in Israel.”

Aside from Hamas, the U.S. must remain vigilant with the ongoing threat of Islamic State. The 2024 Annual U.S. Intelligence Assessment [reported](#) that the regional affiliates of Islamic State and al-Qa’ida are likely to expand in the future and, although terrorism capabilities will fluctuate across Islamic State’s factions, the group will continue to focus on conducting and inspiring global attacks against the U.S. and U.S. interests. The report further indicated that al-Qa’ida and Islamic State, have been motivated by the Hamas attack against Israel, and thus directed their own followers to carry out attacks against Israeli and U.S. interests.

An outpouring of confidence by the global supporters of the Islamic State movement has become apparent. Online [threats](#) against the European

RECOGNIZE THE SIGNS OF TERRORISM-RELATED SUSPICIOUS ACTIVITY



**EXPRESSED
OR IMPLIED THREAT**



PHOTOGRAPHY



**TESTING OR
PROBING OF SECURITY**



**BREACH/ATTEMPTED
INTRUSION**



Source: [U.S. Department of Homeland Security \(2024\)](#)

community coupled with the successful coordinated attack in [Russia](#) on a concert venue foster a potential shift in U.S. thinking about the possible reach of Islamic State. The U.S. intelligence community has elevated concern, especially after [attacks](#) against Taylor Swift concerts in Vienna, Austria, were thwarted in August 2024. Individuals tied to Islamic State made preparatory actions to attack concert venues holding up to 65,000 people inside and potentially thousands more congregating outside the stadium.

In June 2024, the House Committee on Homeland Security [reported](#) that over 370 individuals on the terrorist watchlist had been caught trying to cross the Southwest border since 2021. FBI Director Wray previously [stated](#) in March that dangerous individuals have entered the U.S. illegally at the southern border. In summer 2024, a coordinated sting operation spanning Los Angeles, New York, and Philadelphia [arrested](#) several individuals with suspected terror ties to Islamic State who crossed the border illegally. Wray [commented](#) following the arrest that,

[T]he bigger problem, in my view, is twofold. One, individuals who, when they come in, are either armed with fake documents or snuck in some way or – or, and this is very important, individuals for whom there’s not enough derogatory information in the intelligence community to watch list them yet.

In June 2024, [DHS](#) identified and labeled over 400 immigrants who entered the U.S. from Central Asia as “subjects of concern.” Adding to the concern for an Islamic State-inspired attack, those immigrants were brought in by an Islamic State-affiliated human-smuggling network. The law enforcement community must consider the porous border vulnerabilities that foreign terrorist organizations could exploit as an incentive to carry out terrorist attacks. Additionally, porous and uncontrolled borders continue to

allow transnational criminal syndicates and violent extremist groups to capitalize on the trafficking and smuggling of humans, narcotics, and weapons.

With its primary responsibility of preventing people from entering the U.S. illegally, DHS’s Customs and Border Protection must be able to conduct its operations according to the law without political interference. Promoting seamless information sharing across the intelligence community and law enforcement agency platforms facilitates a successful streamlined process that can aid in border security. This process integrates information systems to enable information sharing at the federal, state, and local levels. Such integration would improve information sharing and safeguard processes and capabilities while strengthening intelligence integration and making it seamless among those in place to protect U.S. citizens.

Heightened Concerns in Afghanistan and the U.S.

[According](#) to the Secretary of Homeland Security Alejandro Mayorkas, speaking before the Committee on Homeland Security, foreign terrorist groups like al-Qa’ida and Islamic State are rebuilding overseas and maintaining worldwide networks of supporters that could target the U.S. The United Nations Security Council released a detailed [report](#) in July 2024 highlighting the threats posed by Islamic State and al-Qa’ida, particularly the “heightened” concerns about the “terrorist threat emanating regionally from Afghanistan.” The report suggests that the most serious threat in the region projecting terror beyond Afghanistan and al-Qa’ida’s enduring presence in the country remains a concern as well. The report further indicates that al-Qa’ida members travel through Afghanistan for “training, recruitment and reorganization activities.... [C]ontinued reorganization and training are judged indicative of the group’s longer-term intent.” Moreover, the report includes the following details that raise concern about al-Qa’ida:

- An ongoing relationship with the Taliban continues to harbor al-Qa'ida members;
- Al-Qa'ida established nine new terrorist camps in Afghanistan in 2024;
- Al-Qa'ida leader Saif al-Adl June 2024 requested that foreign fighters travel to Afghanistan and prepare to attack the West; and
- The current infrastructure and solidified haven in Afghanistan offer opportunities to benefit from al-Adl's call for supporters to migrate to the country.

In addition to external forces looking to infiltrate or inspire, cases of domestic terrorism are on the rise in the U.S. According to DHS reports, there were over 231 domestic terrorism incidents in 2010-2021, with roughly 35% classified as racially or ethnically motivated. Anti-government or anti-authority-motivated violent extremism was the second largest category of incidents at 32%. A 2022 FBI report found that racially or ethnically motivated violent extremists will continue to create the highest threat of executing “lethal violence against [U.S.] civilians,” followed by animal rights and environmental violence, which poses a lesser threat. With individuals inspired, for example, by terror movements and violent public demonstrations, policymakers need comprehensive and objective data to better understand the threats, the factors causing increased threats, and recommendations for change.



Richard Schoeberl, Ph.D., has over 30 years of law enforcement experience, including the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC). He has served in a variety of positions throughout his career, ranging from a supervisory special agent at the FBI's headquarters in Washington, DC, to unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before these organizations, he worked as a special agent investigating violent crime, human trafficking, international terrorism, and organized crime. Additionally, he has authored numerous scholarly articles, serves as a peer mentor with the Police Executive Research Forum, is currently a professor of Criminology and Homeland Security at the University of Tennessee-Southern, and works with Hope for Justice – a global nonprofit combating human trafficking.

According to the Center for Strategic and International Studies, aside from understanding the threats, law enforcement agencies (state, local, and tribal) need further funding and resource assistance to help identify and respond to domestic terrorism before an attack occurs:

The DHS, DOJ, and FBI should continue to review their respective counterterrorism training and resource programs that are provided to federal, state, local, and tribal law enforcement agencies and ensure that such programs include sufficient training and resources in understanding, detecting, deterring, and investigating acts of domestic terrorism.

Understanding the internet's critical role in terrorism, the U.S. and the private sector should pursue groups or individuals that use internet platforms to advocate for violence. Extremists use the internet to raise money, recruit new members, push propaganda, coordinate training, and communicate with one another. Policymakers should continue to require platforms to aggressively take down subjective content that supports terrorism and potentially fosters radicalization. There has been a continuing problem in government action. By the time a trend is identified, and countermeasures are implemented, that trend has likely decreased and is now replaced by a newer threat profile.



Source: CRAIG/Adobe Stock.

Security in and Around D.C. – Following the Informational Dots

By Catherine L. Feinman

In 2021, several people died, approximately [140 police officers were assaulted](#), and countless other physical and psychological injuries went unreported during a single-day catastrophe in Washington, D.C., which was far from a single-day event. Instead, the January 6 attack on the U.S. Capitol was a culmination of malicious activity “dots” that spanned months before the incident. Outside of public view, agencies in and around Washington, D.C., were planning behind the scenes, attempting to connect those dots, and putting plans in place to mitigate the consequences of the escalating violence that was all but inevitable. However, the key players preparing for the First Amendment rally on the Ellipse and the certification of the presidential vote count soon found themselves in the middle of an emergency response.

Amid political controversy, those same agencies have been preparing since 2020 for other election events by using lessons learned and after-action reports to identify and close security gaps. These lessons were shared on September 4-5, 2024, at the D.C. Interoperability Summit, which drew 824 registered attendees from 33 states and 2 territories to address “Preparing for the 60th Presidential Inauguration.” This article provides a glimpse of the discussions at that summit and key action items that agencies

should consider in any jurisdiction to prepare for future threats.

Attack on the U.S. Capitol

So much public attention has focused on January 6, 2021, and the events that followed. However, it is just as important for emergency preparedness and public safety professionals to consider the actions prior to those events. Although agencies typically rely on permit applicants to provide expected crowd sizes and locations, they understand that they are not always accurate. Intelligence revealed an escalation of violence leading up to the certification of 2020 election ballots. So, security planning occurred, but the timeframe was compressed as rally plans changed and threats rapidly evolved. As participants gathered for the [Women for America First](#) rally (known as “[Stop the Steal](#)”), the discovery of [two pipe bombs](#) (placed on January 5 and discovered the next day) near the Republican and Democratic National Committee headquarters changed the dynamics of the day as law enforcement responses shifted and resources depleted. Back at the Capitol, the words “shots fired” soon rippled across agencies, and the violence escalated.

As part of their daily roles, police officers balance law enforcement, public safety, and First Amendment rights. For the first time in

their careers, though, officers at the Capitol building faced threats from all sides as a large protest turned into a riot. Some rioters approached from the left, right, and front. Some maneuvered behind the officers while others climbed up the walls and scaffolding from below or jumped down from above. There were not enough resources to arrest all the rioters on the scene, so law enforcement focused on crowd control, the defense of the Capitol and the legislators inside, and the safety of law enforcement officers. Additional investigators and officers managed potential threats at other locations around the city, including the bomb investigation, crowd control at the Ellipse, and transportation egress.

Some factors that law enforcement did not anticipate that day were the crowd density, cell phone disruptions, unfamiliarity with the Capitol building's layout to outside law enforcement, and the level of involvement in the crowd by active military, police, fire, emergency medical services, pilots, and other professionals sworn to protect communities. Following the event, political rhetoric and social media mis- and disinformation distracted from the facts of that day, and memories have faded with time. However, much still needs to be learned about how the events transpired and what agencies can do to prevent history from repeating in 2024 and beyond.

Reflect on the Past, Plan for the Future

As the 2024 presidential election, certification of votes, and inauguration approach, the 2020 election provides valuable security lessons to learn. Those lessons, coupled with updated intelligence and new factors, provide a roadmap to secure the upcoming election and subsequent special events. Some nefarious tactics will be implemented again, while others will be new. Federal and state agencies continually examine the threat environment and develop plans to

thwart foreign and domestic attacks. [Foreign actors](#) still try to interfere in the cyber domain, which could lead to physical interference. Domestic political violence groups continue to pose physical, cyber, and operational risks within the election infrastructure, such as [threats against election workers](#).

January 6, 2021, was a violent day with severe criminal charges, including [assault on federal officers](#), vandalism and destruction of property, assault on the media, larceny (theft of government property), trespassing, and [seditious conspiracy](#). Some [Capitol breach case](#) investigations are ongoing, with over 1,000 charged to date. The D.C. Interoperability Summit convened a multidisciplinary multijurisdictional group of agency representatives to find actionable solutions to current and future threats. Recommendations those representatives shared included:

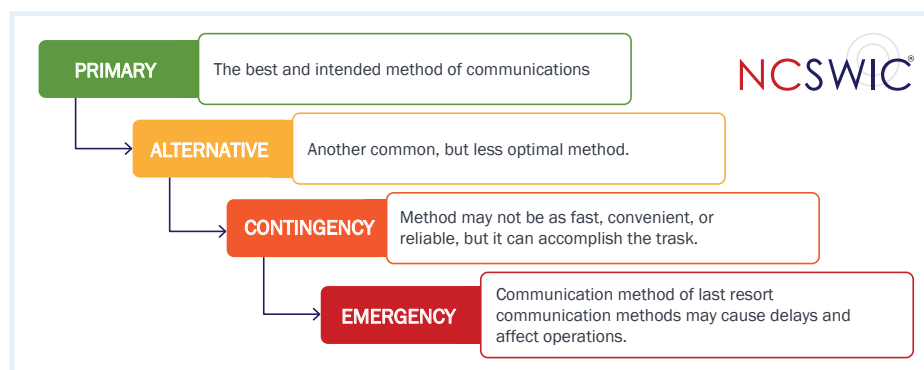
- Develop a [PACE](#) (primary, alternate, contingency, and emergency) communications plan;
- When sending a liaison officer to another agency's command post, make sure that individual has operational experience, is well-versed in the incident action plan, and is authorized to make decisions;
- Diffuse and correct misinformation;
- Be transparent in sharing information with the public;
- Attend planning meetings;
- Include all key stakeholders in training exercises;
- Make exercises realistic;
- Brief executives on resource needs and processes during the planning;
- Consider how to screen for extremism within agencies and organizations;

- Reevaluate personal protective equipment needs;
- Think strategically;
- Cultivate interagency collaboration and partnerships;
- Address the health of responders by developing wellness plans that include mental and physical well-being;
- Understand how the actions of one agency affect other agencies; and
- Take politics out of public safety.

The 2024 presidential election, vote certification, and inauguration are quickly approaching. Agencies across the United States are gathering intelligence, sharing information, and implementing plans to protect communities from domestic and foreign threats related to the U.S. elections. As preparedness professionals already know, the more planning and preparation that occur before an incident, the better the outcome when disaster strikes. One presenter shared the following words of wisdom on September 4, 2024, at the D.C. Interoperability Summit. As agencies prepare



Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 35 years of publishing experience and currently serves as editor-in-chief of the Domestic Preparedness Journal, DomesticPreparedness.com, and The Weekly Brief. She works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in International Business from the University of Maryland, College Park, and a master's degree in Emergency and Disaster Management from American Military University.



Developing and practicing your **Primary, Alternate, Contingency, and Emergency (PACE)** plans will help improve your organization's resiliency and preparations for the next disaster.

PACE produces strategies and redundancies that maintain communications despite disrupted communications networks



See NCSWIC's PACE Products at
cisa.gov/safecom/training-and-exercises



See ICTAP's Offering on PACE at
cisa.gov/safecom/ictapscip-resources

for whatever threats the nation may face, remember that “elections are political, but election security is not.”

Stay tuned for the full after-action report from the 2024 D.C. Interoperability Summit in Fall 2024.

EST



1998

Domestic Preparedness

Real-World Insights for Safer Communities



We Cover It All



Subscribe Today!

www.domesticpreparedness.com/subscribe

