NIST Special Publication 1900
NIST SP 1900-208

NIST Workshop Report

Whole Community Preparedness in Smart Cities and Communities

Michael Dunaway
Cheyney O'Fallon
Wenqi Guo
Thomas Roth

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-208

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 1900
NIST SP 1900-208

NIST Workshop Report

Whole Community Preparedness in Smart Cities and Communities

Michael Dunaway
Cheyney O'Fallon
Wenqi Guo
Thomas Roth
Smart Connected Systems Division
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1900-208

December 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST SP 1900-208
December 2025

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2025-11-14

How to Cite this NIST Technical Series Publication
Dunaway M., O'Fallon C., Guo, W., Roth, T. 2025. Whole Community Preparedness in Smart Cities and Communities. National Institute of Standards and Technology, Gaithersburg, MD, NIST Series SP-1900-208. Publication ID. https://doi.org/10.6028/NIST.SP.1900-208.

Author ORCID IDs
Michael Dunaway 0000-0002-1535-1829
Cheyney O'Fallon 0000-0002-5931-4173
Wenqi Guo 0000-0002-9712-8363
Thomas Roth 0000-0002-9986-7784

Contact Information
michael.dunaway@nist.gov

Abstract

In August 2024, the Smart Connected Systems Division of the National Institute of Standards and Technology (NIST) conducted a workshop entitled, "Whole Community Preparedness in Smart Cities and Communities." The purpose of the workshop was to determine requirements, metrics, and potential improvements to disaster preparedness, post-disaster recovery, and overall community resilience achievable through the integration of advanced digital technologies. The larger objective of the research project is to define the acceptability, feasibility, and general structure of an integrated communications infrastructure to support community disaster planning and response and improve multi-agency crisis communications among local officials and leaders, emergency managers, and the civil population. Over 50 attendees participated, including representatives from academia, federal government, industry, municipalities, and nonprofit organizations. The two-day workshop included keynote addresses, a federal agency panel, presentations, and three breakout sessions involving four teams. Topics addressed by speakers included the evolving nature of emergency management, the role of federal agencies in informing and providing resources for disaster management, achieving balance between technology integration and community engagement, the competing needs of information-sharing and cybersecurity, and the use of digital twins to enhance city operations and community preparedness. Four core themes emerged from the workshop:

(1) the criticality of trust, transparency, and community engagement;
(2) the need for standards in data integration, interoperability, and technology adoption;
(3) the importance of broad participation by community leadership, private citizens, and the business sector as the foundation for whole community preparedness;
(4) the requirement for effective models or templates to structure post-disaster communications, collaboration, and governance.

Based on this initial foundation, the results were presented in two additional workshops at the 2025 Smart Cities Connect Conference in San Antonio, TX, and at the University of Colorado's Natural Hazards Workshop in Boulder, CO. These sessions provided perspectives from an additional 40 participants representing city officials and managers, smart city practitioners, and private sector and university researchers, and reflected real-world experience in technology development and integration by cities and communities and the impacts of natural and technological disasters on cities, towns, and rural communities.

The following outcomes emerged from the series of three workshops and comprise a research agenda to further define requirements, priorities, and resources toward a national Whole Community strategy that would support state and local authorities.

(1) Build a publicly accessible, dual-use communications system for information sharing to enable community collaboration, planning, and coordination during civil emergencies.
(2) Define approaches for strengthening public-private partnerships across communities and develop strategies for coordination and mobilization of community resources.
(3) Conduct scaled emergency exercises that involve elected officials, community leaders, and the private sector and extend through the recovery phase of the disaster cycle.
(4) Establish community and neighborhood Resilience Centers to aid in post-disaster recovery planning and restoration of economic stability, and social and cultural cohesion.

The insights gained from the workshop series are intended to inform future research by NIST laboratories in collaboration with universities, private sector organizations, government officials, and local agencies and community leadership. Ultimately, the goal is to define a strategy toward effective whole community preparedness for cities, communities, and regions against the hazards and threats faced by all.

Keywords
Community resilience; data integration; disaster preparedness; public safety communications; interoperability; public-private partnerships; smart cities; whole community.

Acknowledgements
NIST gratefully acknowledges the contributions made during the August 2024 workshop by the individuals listed in Appendix D, and, as well, the participants at the 2025 Smart Cities Connect Conference and Natural Hazards Workshop who provided additional perspective and insights on disaster resilience, preparedness, and disaster planning based on academic research and real-world experience.

Table of Contents

Preface ..... **v**

1. Overview of the Workshop **1**

1.1. Workshop Goal and Objectives 1

1.2. Workshop Structure and Agenda 2

2. Presentations and Panel Overview **3**

2.1. Introduction to NIST and Workshop Origins 3

2.2. Day 1 Keynote Address: Perspective from State Emergency Management 3

2.3. Federal Agency Panel: FEMA, DHS, CISA 3

2.4. Day 2 Keynote Address: Resilience: Community, Emergence, and Social Capital 4

2.5. CISA Connected Communities Initiative 4

2.6. Use of a Digital Twin for City Operations: Case Study of Coral Gables, Florida 4

3. Breakout Sessions **6**

3.1. Objectives and Process 6

3.2. Breakout Session Questions 7

3.3. Summary of Breakout Session Discussions 8

4. Key Takeaways from Workshop I **15**

4.1. Trust, Transparency, and Community Engagement 15

4.2. Data Integration, Interoperability, and Technology 16

4.3. Governance, Collaboration, and Partnerships 17

4.4. Disaster Preparedness as a Holistic Enterprise 18

5. Workshops II and III: Perspectives from City Officials and Smart City Practitioners **20**

5.1 Question #1 20

5.2 Question #2 22

5.3 Question #3 23

5.4 Question #4 25

6. A Research Agenda for Whole Community Preparedness **27**

Appendix A. Charter Document and Read-Ahead for Workshop Participants **31**

Appendix B. Workshop Agenda **36**

B.1. Agenda Day 1 36

B.2. Agenda Day 2 37

Appendix C. Presentation and Panel Summaries **38**

C.1. Day 1 Sessions and Presentations 38

C.2. Federal Agency Panel 39

C.3. Day 2 Sessions and Presentations 41

C.4 CISA Connected Communities Initiative.....42

C.5. Use of a Digital Twin for City Operations and Community Preparedness.....43

Appendix D. References and Resources 44

Appendix E. Workshop Participants.. 45

Preface

The concept of "whole community preparedness" was originally proposed in 2011 by the Federal Emergency Management Agency (FEMA) with the objective of bringing together different community stakeholders—including private sector entities, local agencies, community groups, and residents—to build disaster-resilient communities.[1] The Centers for Disease Control and Prevention (CDC) adopted a similar collaborative approach to public health in 2013. However, experience gained during the COVID-19 pandemic revealed both gaps and challenges in developing a national strategy for implementation by individual cities and communities. The pandemic's varied impacts highlighted the need for preparedness approaches that are not only comprehensive, but also adaptable to different contexts. Significant research, investment, public engagement, and standardization of organizational structures and communications infrastructure are needed to strengthen the implementation and execution of a whole community approach to disaster management.[2]

Ultimately, the goal of a whole community approach is to provide agency to citizens in times of crisis and enable closer coordination between emergency management and first responders, community leadership (whether elected, appointed, or informal), and the affected civil population. Although some clear prerequisites are required to achieve this goal—such as an information-sharing system, a bottom-up, community-focused organization, and bidirectional communications—more clarification is needed to adequately inform and reinforce such an approach. Improved coordination of both tactics and strategy at the national, regional, and local levels is also required. Cities and communities can play a pivotal role by empowering public discourse and adopting frameworks that promote public safety and facilitate cross-jurisdictional coordination. On the technology side, currently available Information technologies and digital communications (i.e., cell phones and city dashboards) can serve as the foundation for public safety systems that can enable cities, communities and their residents in effectively preparing for and recovering from large-scale events.

Figure 1 from the National Disaster Recovery Framework (NDRF) illustrates the gap in coordination and communications infrastructure that this workshop sought to address. As the red vectors below the NDRF Recovery Continuum illustrate, first responders and emergency managers operate within the organizational structure, doctrine, and dedicated communications networks defined by the National Incident Management System and Incident Command System. In contrast, local authorities, and the civil sector (the dotted blue vector) have no dedicated organizational framework or defined operational protocols or standards, nor the dedicated communications channels that would facilitate coordination of long-term disaster recovery. Though some jurisdictions may have developed individual technology applications and procedures for community or regional coordination, there is no standardized capability for comprehensive situational awareness between response agencies and the community, nor a

[1] Federal Emergency Management Agency. "A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action" (2011). Accessed September 2025. https://www.fema.gov/sites/default/files/2020-07/whole_community_dec2011__2.pdf .

[2] Federal Emergency Management Agency. Pandemic Response to Coronavirus Disease 2019 (COVID-19: Initial Assessment Report. January 2021. Washington D.C. Accessed September 2025. https://www.fema.gov/disaster/coronavirus/data-resources/initial-assessment-report.

formalized or standardized method for communities to identify and prioritize the mobilization of resources during a crisis or civil emergency.

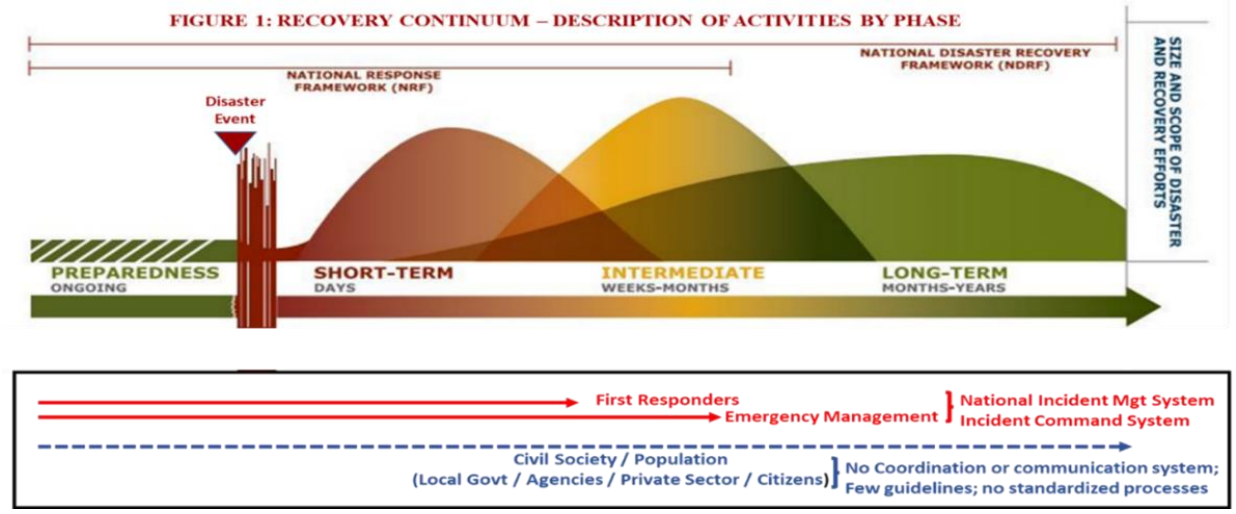

Figure 1. Recovery Continuum defined in the National Disaster Recovery Framework illustrating the challenge for local authorities and the affected population

In 2023, the National Institute of Standards and Technology (NIST) launched a research project within the Smart Cities Infrastructure program to define technology applications, analyses, key performance indicators, and adaptive decision architectures for public safety planning to enable communities to more effectively respond to and recover from large-scale disasters and emergencies. The broader project goal was to develop an information sharing and analysis capability to enable collaborative decision-making between civil authorities, emergency managers, and a community's population. Such a multi-agency, cross-disciplinary capability would allow communities, cities, and regions to evaluate alternative approaches to managing local risks and potential disaster impacts and more effectively coordinate civic capabilities and resources in responding to and recovering from large-scale disasters and civil emergencies.

In order to gain a broad perspective on the challenges of this effort, the NIST project team initiated a technical workshop that brought together a team of senior first responders, emergency managers, members of the academic research community, and city, state, and federal representatives to provide perspective on current and future requirements for enabling communities to more capably manage complex threats to public safety, health, and community welfare. Workshop discussions addressed the acceptability, feasibility, and general structure of an integrated communications infrastructure to support community planning for disaster response and recovery. The workshop was the first step toward defining an organizational and informational infrastructure to improve multi-agency crisis communications and planning and empower local officials and leaders to more effectively manage complex crises.

1. Overview of the Workshop

The Smart Connected Systems Division of the National Institute of Standards and Technology (NIST) conducted the first workshop in Washington, DC, in August 2024, for the purpose of determining requirements, metrics, and potential standards for public safety enhancement, post-disaster recovery, and overall community resilience. The insights gained from this workshop were directed at informing NIST research priorities with the goal of defining a Whole Community Approach to disaster preparedness within the smart cities ecosystem. Over 50 attendees participated, including representatives from academia, federal and state government, industry, municipalities, and nonprofit organizations.

The initial two-day workshop convened on August 27th and 28th, 2024 at Texas A&M's George H.W. Bush School of Government and Public Service in Washington, DC, and was attended by a variety of stakeholders, detailed in the Attendee List (Appendix C). NIST was assisted in workshop planning and logistics by the consulting firm, Energetics, whose team provided facilitation support and prepared the summary report of the workshop

The two-day agenda included keynote addresses, a federal agency panel, presentations, and three breakout sessions (details are in the Appendices). Topics addressed by speakers included the evolving nature of emergency management; the role of federal agencies in informing and providing resources for disaster management; the balance between technology integration and community engagement; the competing needs of information-sharing and cybersecurity; and the use of digital twins to enhance city operations and community situational awareness.

Three breakout sessions involving four separate teams addressed a series of targeted questions with the objective of exploring the components, requirements, and contexts necessary to build a "whole community" communications infrastructure for disaster preparedness and resilience. The first session broadly addressed the foundational aspects (e.g., technical, social, cultural) essential for the support of a whole community approach to disaster preparedness, post-disaster recovery, and general community resilience. The second session examined the technical and operational needs for an integrated communications infrastructure that can facilitate effective community-wide situational awareness. Finally, the third session explored the practical requirements, conditions, and strategies needed to implement these solutions, with a focus on overcoming challenges and fostering collaboration across infrastructure sectors, system components, communities, and jurisdictions.

1.1. Workshop Goal and Objectives

The Whole Community Preparedness Workshop initiated a research effort intended to define the acceptability, feasibility, and general structure of an integrated communications infrastructure to support community disaster planning and response and improve multi-agency crisis communications among local officials and leaders, emergency managers, and the civil population.

Four core themes emerged over the course of the workshop: 1) the essential role of trust, transparency, and community engagement; 2) the fundamental prerequisite for data integration, interoperability, and technological compatibility; 3) the importance of broad participation and leadership in building an approach to whole community preparedness; and 4) the need for

frameworks and standards to build complementary methods of governance, collaboration and partnership to assist in organizing effective management regimes for disaster preparedness and post-disaster recovery at the local level.

The insights gained from this workshop are intended to inform research conducted within NIST's Smart Connected Systems Division and to serve as a foundation for comprehensive community-level emergency planning across the member communities, partners, and organizations of the national smart cities ecosystem.

1.2. Workshop Structure and Agenda

The morning session of the first day began with administrative notes from NIST, Texas A&M University, and Energetics representatives, as well as welcoming remarks from the Executive Director of the Bush School of Government, Lieutenant General Jay B. Silveria, United States Air Force (retired). Dr. Michael Dunaway of NIST's Smart Connected Systems Division provided an introduction to NIST and the overall objectives for the workshop.

Following the introductory remarks, Russell Strickland, Secretary of Emergency Management for the State of Maryland gave the keynote address (summarized in Appendix D.1). Following Secretary Strickland's address, a federal agency panel was conducted, comprised of government agency representatives (named in Section 3). Energetics then provided an overview of breakout session logistics before the day's first breakout sessions focused on foundational aspects of a whole community approach to disaster preparedness, response, and recovery; important elements of those aspects; and challenges associated with implementing such an approach. The rest of the day comprised the two breakout sessions, concluding with reports conducted in a plenary meeting. The final session summarized the day's events and discussions and provided a review of the agenda for Day 2.

The second day of the workshop opened with another welcome message and administrative notes, followed by an introduction of Day 2's focus: implementing an integrated whole community approach to national preparedness. Dr. James Kendra, Director of the University of Delaware's Disaster Research Center, delivered a keynote address on emergent behavior in public crises. Laura Hershon of the Cybersecurity and Infrastructure Security Agency (CISA) then introduced CISA's Connected Communities Initiative. Thereafter, the Energetics facilitators reviewed breakout session logistics before the commencement of the workshop's third and final breakout session. In the afternoon, the breakout groups delivered their respective reports, after which Marc Stolzenberg and Raimundo Rodulfo of Coral Gables, Florida gave a presentation on the implementation of a digital twin for city operations and community preparedness planning. The day concluded with a group discussion held around the topic of implementation strategies for a whole community approach to national preparedness and resilience and the use of technology in achieving the goals of those strategies. Michael Dunaway of NIST offered closing comments summarizing the workshop's results and shared post-workshop next steps before adjournment. The full workshop agenda can be found in Appendix B.

2. Presentations and Panel Overview

Below are high-level accounts of all presentations, including keynote addresses and the federal agency panel. Detailed summaries are available in Appendix E.

2.1. Introduction to NIST and Workshop Origins

Dr. Michael Dunaway, Associate Director for Innovation in NIST's Smart Connected Systems Division, began the workshop by explaining NIST's role as the research laboratory for the U.S. Department of Commerce tasked with advancing measurement science and standards to promote U.S. innovation and competitiveness. Dr. Dunaway shared NIST's definition of a smart city as one that efficiently employs digital technologies to provide prioritized services and benefits to the community, measured according to (1) the number of services and benefits provided; (2) the efficiency in implementation; (3) the assessed quality of those services and benefits; and (4) the alignment of technology adoption toward the goal of achieving community priorities. Dr. Dunaway reiterated that the purpose of a smart city is to provide agency to its citizens, and explained that the goal of the workshop was to define a framework relevant to smart cities for disaster preparedness and community resilience, reinforced by technological, financial, and analytical considerations. He noted the importance of a whole community approach in serving public safety by not only providing agency to citizens in times of crisis but also enabling communication and coordination across cities, regions, and jurisdictions.

2.2. Day 1 Keynote Address: Perspective from State Emergency Management

Secretary Russell Strickland, Secretary of the Maryland Department of Emergency Management, discussed the challenges and opportunities associated with emergency management. He emphasized the evolving and ever-expanding nature of emergency management, illustrating this with the definitional shifts in the phrase "all hazards," which has grown to include school violence, threats to food resilience, and other dangers that have emerged over the years. Secretary Strickland stressed the need for new tools and technologies to address these issues and highlighted artificial intelligence (AI) as a tool to help agencies respond more efficiently in times of crisis. AI re-emerged as a topic of discussion during the Q&A session, and Secretary Strickland mentioned its role in information consolidation, as well as the need to build public trust in AI. Strickland concluded by acknowledging the critical role of technology, while emphasizing the equally critical role of human oversight and a compassionate, data-driven approach in guiding emergency management efforts.

2.3. Federal Agency Panel: FEMA, DHS, CISA

The opening panel discussion provided an opportunity for attendees to hear perspectives from three federal agencies on the concept for an integrated whole community approach to national preparedness. The three panelists included Zachary Smith from the Federal Emergency Management Agency (FEMA), Jeffrey Booth from the Department of Homeland Security (DHS), and David Nolan from the Cybersecurity and Infrastructure Security Agency (CISA).

The panel began with each panelist introducing their respective organizations and relevant projects and initiatives. Mr. Smith gave an overview of FEMA's Strategic Foresight Initiative, which was established in 2023 to help FEMA and the broader emergency management community cope with unprecedented change and uncertainty regarding the future. Next, Mr. Nolan, a member of CISA's Emergency Communications Division, described the division's mission to help manage cybersecurity risks as they relate to critical infrastructure. Mr. Booth, who works at the Science and Technology Directorate of DHS, discussed the directorate's focus on technologies to anticipate or mitigate crises (i.e., "left-of-boom" actions) in support of emergency management, emphasizing the importance of predictive capabilities in regard to regional disasters such as wildfire and flood management.

2.4. Day 2 Keynote Address: Resilience: Community, Emergence, and Social Capital

Dr. James Kendra, Director of the Disaster Research Center at the University of Delaware, delivered Day 2's keynote address, which highlighted the common themes that have emerged in various organizations' attempts to define "resilience." The term has been widely accepted to mean the rapid and efficient recovery of communities in the aftermath of a disaster, coupled with a community's ability to not only survive but thrive in the wake of crisis. Dr. Kendra pointed out that resilience is typically made possible by strong social networks, positive emergent behavior, and creative action/solutions adopted by the population. He illustrated these points with a case study, concluding with a theme that would appear repeatedly throughout the workshop: the need for both technological tools and strong social foundations for efficient community response and recovery from a disaster or emergency.

2.5. CISA Connected Communities Initiative

Laura Hershon, Branch Chief of the CISA Connected Communities Initiative (CCI), opened the presentation with an overview of CCI's purpose, mission, vision, and problem statement. CCI is tasked with helping municipal leaders implement resilient technology by leveraging best practices for risk analysis and mitigation, while bearing in mind the inherent risk of increasing attack surface when adopting smart technologies. She also emphasized the need to create products and resources that promote secure and resilient smart technology deployment, as well as to disseminate information in a bidirectional feedback loop intended to both refine analysis and ensure that the needs of stakeholders are met.

In the Q&A session that followed, Ms. Hershon mentioned CISA's advocacy for voluntary adoption and the leveraging of municipal purchasing power to demand security assurances from technology developers and vendors. Other topics discussed were CISA's capacity for security analytics and developing partnerships with universities as a means to engage students in municipal cybersecurity.

2.6. Use of a Digital Twin for City Operations: Case Study of Coral Gables, Florida

Raimundo Rodulfo, Chief Information Officer of the City of Coral Gables, Florida and Marc Stolzenberg, Advisor to the City Emergency Manager discussed their use of a digital twin to

enhance city operations and community preparedness, with a focus on disaster resilience. Equipped with lessons learned from historic incidents, such as Hurricane Irma, they were able to illustrate a whole community approach to disaster preparedness through the integration of smart city infrastructure, which enabled continuous improvement of response strategies and enhanced community trust and engagement. Through the use of drones, sensors, and fiber optics, Coral Gables has been able to create robust and fast-acting systems designed to aid in public safety, emergency response, and decision-making, while keeping the pulse of environmental conditions and active communication with residents.

3. Breakout Sessions

Three breakout sessions were held over the course of the two-day workshop. Sessions 1 and 2 took place on the first day and Session 3 on the second day. The sessions were structured such that Session 1 was dedicated to brainstorming overarching components of success for an effective whole community approach to disaster preparedness; Session 2 was dedicated to detailing the technical and operational inputs needed to support those components; Session 3 focused on defining the steps needed for implementation of the components that had been identified in Session 1. Further details on each session and their respective focuses, beginning with the sessions' respective objectives, are provided below.

3.1. Objectives and Process

The stated objectives of the breakout sessions were as follows:

- Session 1
  - Compile a comprehensive list of aspects of a whole community communications infrastructure that contribute to disaster preparedness and resilience.
  - Prioritize the top aspects of a whole community communications infrastructure.
- Session 2
  - Explore prioritized aspects in detail, identifying components, benefits, and challenges.
  - Identify critical technologies, mechanisms, and standards for implementation.
- Session 3
  - Define the key steps for implementing the communications infrastructure across various levels of government and community.
  - Align the implementation strategy with federal, state, and local priorities to ensure broad-based support and collaboration.

Each breakout room was managed by a facilitator and a notetaker. The facilitator led participant discussion via a combination of projected PowerPoint slides containing the questions assigned to each session, real-time inputs (generated by participant discussion) compiled into charts provided in the slides, and guiding questions posed when and where necessary. In addition to engaging in discussion, the participants themselves were tasked with filling out index cards with proposed foundational aspects for Session 1; technical and operational elements for Session 2; and implementation requirements for Session 3. The cards were then pinned onto storyboards for comment by the entire room, after which participants prioritized (or otherwise organized) them. The notetaker captured as much of the discussion as possible.

Each of the three breakout rooms addressed the same set of questions, and breakout room assignments remained static for the duration of the workshop. To maintain a balance of perspectives across the breakout rooms, participants were roughly evenly distributed across rooms by representation of federal government, state and local government, academia, private

sector, and nonprofit sectors. After each breakout session had concluded, a designated presenter (sometimes the facilitator, sometimes a participant) from each room summarized key points from the group's discussion for all workshop attendees in the main plenary room.

3.2. Breakout Session Questions

The questions addressed during all three breakout sessions are outlined below. (Where "we," "our," or "us" appears in the questions, it refers to the broader community of people working on a whole community approach to preparedness, and not NIST specifically).

3.2.1. Breakout Session 1: Defining boundaries and components

The focus of Breakout Session 1 was on taking a wide view of existing "whole community" approaches to disaster preparedness, zeroing in on the components and criteria that lend strength to these systems, and then using those insights to begin constructing a list of foundational aspects deemed essential to the success of such an approach. The questions posed to fuel this discussion are listed below:

- What *foundational aspects* (e.g., technical, social, cultural) are essential to support a whole community approach to disaster preparedness, response, and recovery?
- What are the *essential components* and criteria for a robust communications infrastructure that supports whole community disaster preparedness and resilience?
- What *existing resources, technologies, and practices* contribute to the development of an integrated communications infrastructure for disaster management?
- What critical concepts are currently missing that need to be addressed to achieve a whole community approach?
- Among the aspects identified on the boards, what are the top four *most important* and top four *most feasible*?

3.2.2. Breakout Session 2: Identifying Specific Characteristics and Requirements

Breakout Session 2 focused on taking a closer look at the foundational aspects identified in Breakout Session 1 and determining the specific technical and operational elements needed to support their successful implementation. Benefits, as well as challenges, associated with the identified aspects were also addressed. The following questions framed this discussion:

- What are *technical and operational elements* of an integrated communications infrastructure that would support whole community preparedness and resilience?
- What specific *technologies and processes* are necessary for this aspect, and how can they be effectively integrated into the existing infrastructure?
- What *benefits* does this aspect provide to a whole community approach?

- What are the potential *challenges* associated with this aspect, and how can those challenges be addressed in the system's design?

3.2.3. Breakout Session 3: Implementing Solutions

The focus of Breakout Session 3 was on identifying conditions and incremental steps needed to implement the foundational aspects identified in Breakout Session 1. This session included deliberations over the types of technologies and other forms of support needed to ease implementation of the foundational aspects. Potential obstacles to implementation were also addressed. The questions posed to fuel this discussion are listed below:

- What are the *requirements and conditions for implementing* a whole community approach for national preparedness and resilience? What are the technologies, infrastructures, doctrines, and strategies to do so?
- What are the *essential steps* required to implement an integrated communications infrastructure that effectively connects federal, state, and local governments with community stakeholders?
- What are the *critical technologies, mechanisms, and standards* to leverage for implementing the prioritized aspects and elements of the communications infrastructure identified in the previous sessions?
- What are the biggest *obstacles* to implementing a whole community approach at a national level? How can they be addressed?

3.3. Summary of Breakout Session Discussions

Workshop attendees, whose experience spanned public, private, and community sectors, brought a wide range of insights to the discussion of whole community preparedness. While the breakout session discussions remained at a high-level, they provided valuable foundational perspectives on community resilience, data interoperability, and access to technology. These themes aligned with the goals of the workshop by emphasizing the need for community engagement and participation, the importance of shared communication standards, and the need for collaboration across sectors.

This section presents key points and core themes identified in participant discussions, categorized into the three primary areas defined above: 1) foundational aspects of community preparedness, 2) technical and operational elements of an integrated communications infrastructure, and 3) practical approaches to implementing solutions. While these points reflect the views of individuals rather than a consensus or official perspective from NIST or other federal agencies, they highlight significant challenges and opportunities for future planning, including the essential role of interoperability standards, cross-sector partnerships, and resilient infrastructure in advancing a whole community approach to preparedness.

3.3.1. Foundational Aspects for a Whole Community Approach

A whole community approach to preparedness centers on trust, collaboration, and the equal participation of all community sectors, including vulnerable populations. Discussions highlighted that fostering community-wide resilience requires building trusted networks and providing common access to preparedness resources. Engaging underserved populations and bridging social divides were viewed as crucial for effective preparedness and response.

- **Foundational Aspects of Trust and Collaboration:** Participation of vulnerable populations is essential to a whole community approach and ensures that engagement reaches all community sectors, especially those who may be least prepared. Comprehensive preparedness requires that every population segment has access to the resources and information they need to respond effectively during a crisis.

  Building trust through community networks and local leadership is fundamental to resilience. Trusted relationships provide a foundation that supports consistent and reliable communication, fostering a sense of security and cooperation among community members before, during, and after emergencies.

> **Equal access and engagement across all community sectors.** Participants emphasized that preparedness must include everyone, especially vulnerable populations, to create a resilient community approach. One attendee noted, "Preparedness must reach beyond traditional methods to include those often missed in emergency communications, or we risk leaving significant gaps in our response."

- **Technology as a Support System:** Emerging technologies, like AI and crowdsourced data platforms, have a significant role in both proactive and reactive disaster management. Integrating these tools allows for better prediction, response, and adaptation to unfolding events, enhancing the overall effectiveness of preparedness efforts.

  Social media platforms are valuable for disseminating emergency alerts, providing a fast and accessible way to reach large audiences. Real-time feedback systems, which include crowdsourced and community-sourced data, offer essential situational awareness, allowing responders to adapt to conditions as they evolve.

  Older analog technologies, such as AM/FM radios, landline telephones, and resilient telecommunications infrastructures, remain vital as backup systems during disasters. These more traditional methods ensure that critical information can be accessed when newer digital technologies might fail, helping to maintain communication with all community segments.

- **Effective Communications Strategies:** Clear, action-oriented messaging that can be understood across demographics is a crucial element of effective crisis communications. Making information accessible and easily actionable ensures that community members can respond appropriately during a crisis, regardless of their background.

There is a need for bidirectional, multimodal communication that combines human and electronic systems. This approach supports not only the dissemination of information but also the collection of feedback and helps refine response efforts and improve community engagement.

- **Social and Cultural Resilience:** Developing cultural competence within disaster plans enhances engagement, especially with historically underserved communities. Recognizing the unique needs and values of groups within a community strengthens the effectiveness of response efforts and promotes broad-based community preparedness.

  Established community networks, such as local non-profits and faith-based organizations, play a crucial role in building trust and engagement. These organizations are well-positioned to connect with their communities and foster a culture of resilience that supports the goals of preparedness initiatives while building trust within the community.

  Neighborhood networks that operate during both routine and emergency situations reinforce community resilience. These networks encourage collaboration and shared responsibility, making them invaluable resources for supporting local preparedness and response efforts.

> **Building Trust within Local Networks:** Trust-building with local leaders and established community networks was highlighted as essential for resilience. "Experience shows that trust is best built before a disaster occurs—through local, credible sources that community members rely on," remarked one participant.

3.3.2. Technical and Operational Elements of an Integrated Communications Infrastructure

Creating a resilient and integrated communications infrastructure is essential for coordinating disaster response efforts across sectors. Key elements include standardized data-sharing protocols, interoperable systems, and robust data governance to prevent information silos. Participants emphasized that both high-tech and low-tech communication channels are needed to maintain accessibility and functionality during crises.

- **Data and Communication Standards:** Standardized data exchange and communication protocols are essential to bridging gaps between systems and sectors. Without these shared standards, interoperability is limited, and collaboration becomes challenging, especially when multiple agencies and organizations must work together—often across adjacent jurisdictions—during a disaster.

  Data stewardship and governance structures play a vital role in ensuring compliance with data-sharing protocols and preventing silos. These structures help maintain a seamless flow of actionable information, allowing data to be accessible and reliable across different sectors and systems.

Ensuring interoperability between technical systems, including telecommunications, data platforms, and emergency response tools, is critical for effective disaster response. When data formats and systems are inconsistent, decision-making can be delayed, impacting the efficiency and effectiveness of crisis response efforts.

> **Standardized Communication Protocols for Interoperability:** Participants emphasized that interoperable data-sharing standards are necessary to streamline collaboration across sectors. As one attendee stated, "Without standardized protocols, we encounter barriers in communication that slow down critical decision-making,".

- **Trust, Message Fatigue, and Response Challenges:** Overcommunicating or sending too many irrelevant or non-actionable messages can lead to "message fatigue," reducing public responsiveness to important alerts. A well-balanced communication strategy is needed to ensure that essential messages are clear and prompt appropriate action without overwhelming the community.

  Trust in government communication is vital, as it influences public response and compliance during emergencies. Trust takes time to build and can erode quickly, so maintaining transparent, reliable communication is essential for effective engagement and community resilience.

  Building trust in data from both public and private sources improves decision-making during disasters. When communities trust the sources of information, skepticism is reduced, and collaboration across sectors is strengthened, making for a more unified response to crises.

> **Trust in Cross-Sector Data-Sharing:** Trust in data sources from both public and private sectors was considered key for effective decision-making. "For data to inform action, communities need to trust that it’s reliable and handled responsibly," said one participant, emphasizing the need for transparency and integrity in data management.

- **Infrastructure Redundancy and Resilience:** Resilient infrastructure, including analog fallbacks to digital systems, are crucial for maintaining functionality during disasters. This redundancy ensures that essential communication channels remain operational, even if primary systems fail or are otherwise compromised.

  Flexibility and adaptability in infrastructure design allow systems to respond to evolving threats effectively. In times of crisis, adaptable infrastructure is essential for continuous operations and quick recovery, supporting community resilience and minimizing disruptions.

> **Redundancy with Both High- and Low-Tech Solutions:** Ensuring system resilience requires a combination of advanced and traditional technologies, including digital and analog backups, as noted by several attendees. "In the event that newer systems fail, fallback options like battery- or solar-powered AM/FM radios keep vital information accessible to everyone," explained one participant.

- **Cross-Sector Involvement:** Public-private partnerships significantly enhance disaster response capabilities by pooling resources and operational support from multiple sectors. The private sector plays a critical role in complementing public resources, particularly when addressing supply chain needs and infrastructure management.

  Incorporating partnerships, such as FEMA's National Business Emergency Operations Center (NBEOC) and Voluntary Organizations Active in Disaster (VOAD), strengthens operational coordination and resource-sharing across sectors. These partnerships enable streamlined, coordinated efforts in disaster preparedness and response.

  Ensuring universal access to technology and communications systems remains a challenge, especially across the numerous communities and neighborhoods that characterize modern cities. Addressing these disparities is crucial for building a resilient regional approach to disaster preparedness, as common access ensures that all community members can stay informed and connected during emergencies.

3.3.3. Implementing Solutions and Overcoming Obstacles

To advance whole community preparedness, participants discussed practical solutions for enhancing resilience and overcoming barriers such as funding limitations and slow technology adoption. They highlighted the potential of pilot programs, public-private partnerships, and education initiatives to promote community engagement and ensure preparedness measures are actionable. Addressing these challenges will require collaboration across government, private, and community sectors.

- **Technological Advancements and Integration:** Technologies such as digital twins, artificial intelligence, and geographic information systems (GIS) offer innovative solutions that support real-time decision-making and situational awareness. These tools provide critical insights that help communities better understand and prepare for potential disaster impacts, ultimately enhancing overall resilience.

  Developing systems that allow for cross-sector interoperability ensures that a range of data sources can be integrated and used effectively during emergencies. By enabling seamless data-sharing across sectors, these systems improve the coordination and responsiveness of emergency management efforts.

Building foundational data layers for disaster preparedness is essential for creating an informed response framework. These data layers integrate critical geographic, demographic, and infrastructure information, helping responders and local authorities to understand both physical and social vulnerabilities within the community.

> **Building Foundational Data Layers for Disaster Preparedness:** Participants emphasized the importance of establishing foundational data layers, particularly for the integration of GIS and digital twins. These technologies provide essential insights for real-time decision-making and situational awareness, helping communities understand the physical and social dimensions of preparedness.

- **Overcoming Barriers to Implementation:** Limited funding, slow adoption rates, and risk aversion (especially among state and local government) are common challenges to implementing new technologies and communications infrastructures. These barriers can delay the deployment of critical solutions, making it essential to secure resources and address concerns early in the planning process.

  The decentralized nature of U.S. communications systems presents coordination challenges, as local, state, and federal entities may have differing priorities and capacities. Standardized frameworks and governance models are needed to align these various efforts and ensure a unified approach to disaster preparedness.

> **Addressing Funding and Adoption Barriers:** Limited funding and slow adoption were recognized as major barriers, particularly at the local level. "Without sustained support, we risk delays in deploying critical technologies where they're needed most," observed one attendee.

- **Community Engagement:** Involving communities early in planning processes fosters better engagement and results in preparedness strategies that reflect local needs. When community members are active participants in planning, they are more likely to feel invested in and prepared for emergency response efforts.

  Building redundancy into both digital and analog systems helps keep communication channels open and functional during crises. A resilient communication structure allows communities to stay connected and informed, even when primary systems are disrupted.

  Leveraging established frameworks like FEMA's National Incident Management System, Incident Command System, and the National Disaster Recovery Framework aligns local preparedness efforts with national standards. This alignment improves coordination and interoperability across government agencies and community organizations, strengthening overall disaster response capabilities.

> **Identifying Essential Steps from a User Perspective:** Attendees felt that NIST would benefit from understanding the essential on-the-ground steps from the perspective of end-users to make its frameworks more actionable. “NIST’s role should be about listening and adapting,” noted one participant, emphasizing that a user-centered approach could improve implementation success.

- **Data-Sharing and Collaboration:** Improved data-sharing between sectors and government agencies is critical for effective disaster response, yet issues of trust and data stewardship remain significant hurdles. Addressing these concerns is necessary to promote openness and ensure that data shared across sectors can be trusted and effectively used.

  Public-private collaboration is essential, with mechanisms like open data standards enabling more seamless integration of information across organizations. By working together, public and private entities can support a more comprehensive, unified approach to community resilience.

> **Public-Private Partnerships as Catalysts for Resilience:** Participants pointed to the benefits of collaboration with private partners, who bring essential resources and support for disaster preparedness. "The private sector plays a key role in filling gaps that public resources alone can’t address," noted a participant, highlighting the value of coordinated efforts.

- **Education and Training:** Community members benefit from training that enhances their understanding and ability to act on emergency communications. Workshops, educational campaigns, and grassroots networks build community literacy around disaster preparedness, empowering individuals to take action during emergencies.

  Regular education, training, and collaborative exercises on data-sharing protocols ensure that all stakeholders can effectively use and share critical information. Familiarity with these systems and practices improves coordinated responses during emergencies, strengthening community readiness.

4. Key Takeaways from Workshop I

The workshop discussions emphasized several core themes as foundational elements for advancing a whole community approach to disaster preparedness. These themes reflect both the social and technical aspects of resilience, highlighting the need for collaborative frameworks, adaptable technologies, and holistic planning and practices that includes all segments of the community. Each takeaway underscores the importance of aligning community engagement, data integration, and cross-sector partnerships to foster a cohesive and effective preparedness strategy. The essential themes of the breakout discussions included:

- **Trust, transparency, and community engagement** focused on the human side of preparedness.
- **Data integration and technology**, with emphasis on interoperability and innovation.
- **Cross-Sector collaboration** to ensure the needs of all communities, districts, neighborhoods, and private sector entities are met.
- **Governance and partnerships** that prioritize collaboration and strive toward standardized approaches to preparedness and response.

> **Transparent Communication to Build Public Trust:** Transparent practices around data use and dissemination are foundational to building trust with the public. "When people understand where the data comes from and how it's used, they're more likely to trust it and act on it," one participant noted.

4.1. Trust, Transparency, and Community Engagement

Trust between authorities and communities is essential for effective disaster preparedness and response. Transparent communication and genuine involvement of community members in both planning and implementation phases help foster trust and ensure that policies reflect the needs of the people they serve. By building these trusted relationships, authorities can enhance resilience, empower communities to act, and promote a culture of preparedness.

- **Building public trust and fostering transparency in communication and data usage:** Trust relies on clear, consistent messaging that makes complex information understandable and actionable. Transparency around data collection, usage, and sharing helps reduce skepticism and enhances public confidence in disaster preparedness efforts.

> **Trust and Data Vetting:** Trust was seen as foundational to data management, and attendees felt that NIST's authority in vetting information could reinforce public trust in data-sharing and usage. One participant commented, "Above all, trust is the key. If NIST can help with validation of the information provided, it will go a long way toward reassuring communities that the data they rely on is credible."

- **Engaging the community in co-designing policies and response systems:** Involving community members in the design of policies and protocols enables more responsive, relevant approaches. Collaborative planning helps ensure that preparedness strategies align with local values and needs, strengthening community buy-in and engagement.

> **Pilot Projects for Real-World Testing:** Pilot programs were seen as invaluable for testing new resilience strategies on a smaller scale before broader rollout. "Pilots allow us to refine approaches and troubleshoot potential challenges before implementing them in a real crisis," shared one attendee.

- **Feedback loops, After-Action Reviews (AARs) and Lessons Learned offer opportunities for learning from past experiences to improve future responses:** Incorporating feedback from previous disasters and routine exercises allows authorities to adapt strategies based on real-world outcomes. This ongoing learning process not only improves preparedness but also demonstrates a commitment to evolving and meeting community expectations.

> **Feedback Loops for Continuous Improvement:** Participants emphasized that learning from past experiences is essential to strengthen future responses. "Every event teaches us something; incorporating feedback helps us adjust our strategies and improve preparedness over time," shared one attendee.

4.2. Data Integration, Interoperability, and Technology

The integration of technology and data, along with interoperable systems, is critical for effective disaster management. By enabling seamless data-sharing across public and private sectors, communities can enhance coordination and situational awareness. Advanced technologies such as artificial intelligence, predictive analytics, and digital twins provide actionable insights that support proactive decision-making and robust, reliable communication channels during crises.

- **Interoperability of systems and data integration across public and private sectors:** Unified data standards allow information to flow smoothly across agencies and organizations, reducing delays and enabling a coordinated response. Interoperable systems ensure that critical data is accessible to all stakeholders when it is needed most.

> **Interoperability as a Cornerstone of Effective Response:** Interoperable systems were viewed as critical for enabling seamless data-sharing across sectors. "When our systems communicate effectively, we can make

> faster, more informed decisions that ultimately save lives," an attendee emphasized.

- **Resilient technology infrastructure and innovative solutions like Artificial Intelligence (AI), Internet of Things (IoT) Sensors, and Digital Twins:** Investing in resilient and redundant communications systems, IoT-networked sensors, and digital twin technologies, ensure continuous connectivity during emergencies. These tools create real-time situational awareness and foster rapid decision-making, enabling a more adaptive response to evolving disaster scenarios. Advanced analytics provide predictive insights into community vulnerabilities and resource needs, allowing for data-driven preparedness strategies. AI-driven models can assess risks and enable proactive interventions, helping communities stay ahead of potential crises.

> **Advanced Technologies for Enhanced Situational Awareness:** Technologies like AI, IoT, and GIS were highlighted for their ability to provide real-time insights into risks and infrastructure vulnerabilities. "AI allows us to predict and respond to evolving threats with more precision, which is critical in a crisis," said one participant.

- **Redundant channels to ensure reliable communication methods:** Redundant systems, including both digital and analog options, provide multiple ways to communicate essential information. This redundancy is essential for reaching all community members, regardless of technology or broadband access, during high-stakes emergencies.

4.3. Governance, Collaboration, and Partnerships

Effective disaster preparedness relies on strong governance frameworks, collaborative partnerships, and standardized protocols that bring together resources from across sectors. Public-private partnerships and interagency collaboration ensure that disaster response efforts are well-coordinated, while standardized governance models enable cohesive actions across jurisdictions. Together, these elements provide a structured approach that strengthens community resilience.

- **Public-private partnerships and the role of the private sector in disaster resilience**: Private sector involvement is essential for effective preparedness, from providing technical expertise to supplying critical resources. Collaborative partnerships with businesses and non-profit organizations help fill gaps in public resources and improve response capabilities.
- **Collaborating across sectors to enhance access to critical resources and technologies**: Cross-sector collaboration ensures that communities have access to the tools, information, and support needed during crises. By pooling resources and expertise,

public, private, and non-profit partners can create a more resilient disaster response infrastructure.

- **Establishing standardization and governance frameworks to ensure cohesive disaster response across jurisdictions**: Standardized governance models promote coordinated disaster response efforts at local, state, and federal levels. These frameworks allow for a unified approach to preparedness, enabling jurisdictions to share resources, data, and protocols effectively.

> **Leveraging Existing Standards, GCTC, and Smart Cities:** The group highlighted NIST's Global Community Technology Challenge (GCTC) Strategic Plan and existing smart city standards as valuable resources for aligning resilience efforts across sectors. By leveraging these standards, participants believed that communities could benefit from a tested, strategic approach to building interoperable smart city solutions.

4.4. Disaster Preparedness as a Holistic Enterprise

Disaster preparedness must be holistic in its approach to engagement within a community, with special attention given to underserved communities that may face greater exposure to disaster impacts and challenges in accessing resources. Ensuring uniformity in disaster response requires addressing the digital divide, supporting communities with low digital literacy, and making sure that vital information and services are available to all populations.

- **Ensuring access, particularly for marginalized and underserved communities:** Effective preparedness requires tailored outreach that addresses community needs with common access to resources, such as emergency information and response services, to ensure that all community members are supported during a disaster.
- **Addressing the digital divide and supporting communities with low digital literacy and limited access to reliable infrastructure:** Many communities face barriers to digital access, including limited internet connectivity or low digital literacy. Preparedness efforts must consider these challenges by providing alternative communication methods and resources that are accessible to all.

> **Addressing the Digital Divide:** Ensuring that emergency information reaches all community members, especially those with limited digital access, was recognized as a core component of community preparedness. "If we only rely on digital communication, we're excluding whole groups that don't have regular internet access," one attendee remarked.

- **Promoting common access to preparedness resources across social, technical, and cultural dimensions:** Holistic preparedness considers social, cultural, and linguistic

differences. Disaster plans that accommodate these differences foster enhanced engagement, empowering all community members to participate in preparedness efforts and respond effectively.

5. Workshops II and III: Perspectives from City Officials and Smart City Practitioners and Members of the Disaster Research Community

Workshop II & III Structure and Objectives

Based on the outcomes of the initial workshop in August 2024, two brief but more focused workshops were conducted in April 2025 at the Smart Cities Connect (SCC) Conference in San Antonio, Texas on 16 April 2025, and at the Natural Hazards Workshop in Boulder, Colorado in 16 July 2025. The purpose of these two sessions was to gain additional perspectives on the Whole Community Preparedness concept from city officials, community leaders, and technology developers with experience in integrating public safety-related technologies within their communities, and from members of the academic research community who specialize in studying real-world disasters and mitigation strategies, and the impact of civil emergencies on cities, communities, and populations. The following section provides a summary of the observations gained during those two sessions with continuing emphasis on the relevant issues for developing and implementing smart technologies and solutions to enhance public safety and community resilience. The workshops were organized around four questions to focus discussions on potential practical applications that could help achieve the goal of Whole Community Preparedness as defined in this project.

1. What capabilities should be developed to support communities in times of disaster or civic emergency?
2. Should a community-focused decision support and information sharing system be designed as:
   - ❑ A dedicated system to be reserved for local/civic preparedness, response, and recovery only? OR
   - ❑ A dual-use system having utility for both Blue-Sky (normal) and Gray-Sky (crisis) days? [If the latter, what capabilities should the Blue-Sky function incorporate]?
3. What Key Performance Indicators (KPIs) should be developed and integrated into a community decision support system for disaster preparedness and recovery?
4. How should operational considerations (efficiency of command/control/coordination) be balanced with civic considerations such as transparency/access/equity and maintenance of public trust?

The following sections summarize the findings from Workshops II and III.

5.1 Question #1

What capabilities should be developed to support communities in times of disaster or civic emergency?

To protect residents, preserve critical infrastructure, and position the community for a safe and efficient post-disaster recovery, communities must develop a range of integrated capabilities for communication of vital information and coordination of community resources and talent. Experts emphasized the importance of shifting focus from reactive emergency response toward proactive preparedness and mitigation with an emphasis on “preparing for recovery. This includes investing in decision systems and predictive analytics for scenario planning and training, and logistics management and allocation to ensure the right resources reach the right place at the right time.

The use of geographic information systems (GIS) mapping tools and geographic intelligence in planning was highlighted as a critical capability.

Technical and engineering aspects such as a resilient power grid with backup power supplies and capability to charge EV-based emergency vehicles and public transport were identified as critical.

Connectivity and communication infrastructure were identified as foundational to coordination of community response and recovery. Maintaining traffic control and coordination during public evacuation regardless of interruptions in local electrical power was also cited as essential. Experts stressed the need for robust, redundant communications through localized mobile towers and analog or low-tech alternatives as survivable back-up systems—including rural or underserved areas. Equally important is ensuring that communication is trusted, multilingual, and accessible across various levels of technology reliability.

A standardized opt-in community outreach protocol should be developed to support community planning and response. The protocol should be designed to use regionally accessible social media, alongside official public channels. Geo-fencing of local communications channels would aid in facilitating trusted, community-oriented management of disaster recovery. Community-wide training should be conducted that includes both civic and private sector leadership and extends past the response phase (the purview of professional emergency management and first responders) and incorporates and tests recovery strategies that engages the whole community. Establishing a digital twin capability for local and regional planning and training would greatly enhance the community's ability to visualize potential risks and plan for mitigation strategies. Systems should be used routinely to ensure elected officials and the general public are familiar and adequately trained (perhaps via digital twin-based simulations and exercises) to respond capably in a disaster.

On the non-technical side, participants cited the value of social capital and community-led planning. Experts pointed out that social preparedness—regular community engagement, local leadership structures, and clear, authoritative guidance—can be as impactful as hard infrastructure. Programs that foster local networks, such as community civic organizations that sponsor events and dinners following a tabletop exercise, were seen as effective tools for building resilience, a sense of common purpose, and trust within a community. Cities should identify and train neighborhood or district "ambassadors" to serve as local points of contact during crises or emergencies and establish community engagement channels and coordination sites or hubs. Residents should be kept informed about local government's efforts to manage crises affecting the population, while protecting personally identifiable information (PII) and the personal safety of victims during a disaster. Frequent public messaging before and during a crisis is important for maintaining the trust of the civil population in the community's or city's leadership.

Finally, the integration of private sector capabilities and critical infrastructure into emergency planning was seen as essential. Since private entities often own and operate much of the infrastructure, embedding their capabilities into the city's planning and response framework ensures a more holistic and coordinated effort. Across all phases—mitigation, preparedness, response, and recovery—clarity on roles, shared resources, and trusted information flow is vital for effective community support. Community planning should emphasize measures to maintain supply chains down to the neighborhood level through both big-box suppliers and local grocers,

pharmacies, and convenience stores. The role of small business in spearheading local economic recovery post-disaster was identified as a community resilience strategy that should be emphasized. Resilient access to currency—whether through secure Automatic Teller Machines (ATMs) with independent power supplies, or through a regionally accessible crypto currency for emergency supply—was offered as an important means to speed post-disaster recovery.

Summary points from Question #1

What capabilities should be developed to support communities in times of disaster or civic emergency? i.e., What do smart cities and communities need to improve resilience and preparedness for recovery?

- **A common information sharing and planning application focused on proactive mitigation and preparedness for recovery rather than reactive emergency and disaster response**
- **Scenario planning and community exercises based on predictive analytics of local risks and hazards and potential outcomes if mitigation/preparedness goals are not achieved**
- **Use of GIS mapping tools and digital twins with public access to help community leadership in making the case for personal, community, and regional planning and resilience initiatives**
- **Assured ability to maintain local communications infrastructure and connectivity with optional "opt-in" feature for community outreach and mandatory "opt-out" feature for emergency notifications**
- **Resilient grid with backup power supplies to maintain community communications, traffic control, and capability to charge EV-based emergency vehicles and public transport.**
- **Positive efforts to include non-elected leadership and public representatives in emergency planning and to build and enhance social networks and communications channels**
- **Incorporation of private sector capabilities and resources in local and regional planning**

5.2 Question #2

(a) Should a community-focused information and decision support system be designed as

- **A dedicated system to be reserved for local/civic preparedness, response, and recovery only?**
- **A dual-use system having utility for both Blue-Sky (normal) and Gray-Sky (crisis) days?**

(b) If dual use, what functions should be incorporated into a community operations system or portal (e.g., public access to city services; licensing and permitting; traffic cameras; support to business operations, etc.)?

This expert group strongly supported the development of a dual-use community information and decision support system—one that functions during both normal operations (blue-sky days) and emergencies (gray-sky days). The key advantage of this approach is that it allows communities to build familiarity with the system through frequent use in everyday life, making it more effective and trusted when crises occur. However, the group highlighted the need for clear modes of

operation, such as a visual or audible signal (e.g., a "red button" or special alert) to indicate a shift into emergency mode, ensuring the system garners the necessary attention and urgency when needed.

At the same time, participants noted that not all functions should be dual-use. For example, emergency alert systems may lose effectiveness if overused in non-crisis times due to notification fatigue. They emphasized the need for priority access and preemption mechanisms in emergencies—similar to FirstNet's emergency prioritization of broadband communications for first responders. The system should also be opt-in with predefined roles, ensuring residents and responders know their responsibilities and can act quickly during disasters.

Participant conversations emphasized two-way communication and community agency as vital elements—allowing residents not just to receive information but also to influence what they get and how. This supports community buy-in and increases trust, especially when supported by multilingual capabilities and analog options for when digital systems fail. Participants also stressed the importance of geofencing and hyper-local alerts, especially for visitors or transient populations, and advocated for leveraging existing platforms like 3-1-1 systems and smart kiosks to distribute relevant information.

Lastly, cross-jurisdictional challenges were flagged as a barrier. While dual-use systems are ideal, they can be hard to implement when multiple jurisdictions are involved—particularly if no routine collaboration or information sharing existed prior to a regional emergency or disaster. In such cases, some argued for designing systems with adaptable emergency-only layers or use cases that work across boundaries without requiring full unification of day-to-day operations.

Summary Points from Question #2:
Should a community-focused information and decision support system be designed as:

- ❑ **A dedicated system to be reserved for local/civil preparedness, response, and recovery only? OR**
- ❑ **A dual-use system having utility for both Blue-Sky (normal) and Gray-Sky (crisis) days?**

⇨ ***Near unanimous agreement on a dual-use system. Rationale: availability 24 x 7 x 365, which:***

- **Builds community familiarity with the system prior to its use in an emergency**
- **Uses an invested resource to benefit the community on a routine basis rather than episodically**

What characteristics should be incorporated into a dual-use community operations system or portal?

- **Dedication to two-way communications with public—not transmit-only from emergency management**
- **Some functions clearly activated only during emergencies (not dual-use) e.g., iPAWS / FirstNet**
- **Active engagement with community and public to build familiarity, trust, and operational awareness (e.g., a city dashboard with open access by the public and civic-focused information delivery)**
- **Dedicated, standardized coordination across jurisdictions and regions and between/within cities**

5.3 Question #3

What Key Performance Indicators (KPIs) should be developed and integrated into a community information sharing and decision support system for disaster preparedness and recovery? (i.e., what do we measure, and how do we measure it?)

Workshop participant responses reflected a broad and thoughtful approach to developing Key Performance Indicators (KPIs) for community information sharing and decision support systems in disaster preparedness and recovery. A major theme is open access and human-centered design—suggesting KPIs should measure not only overall system performance but also the distribution of outcomes across different neighborhoods and demographics. Rather than using only high-level citywide averages, the group recommended disaggregating data to identify how various communities are affected and whether outreach efforts are truly reaching targeted populations.

Another important dimension emphasized the effectiveness of communications and engagement. KPIs should assess who receives information, who understands it, and who takes action as a result. Beyond message delivery, attendees stressed the importance of measuring participation in educational efforts exercises, and drills, and identifying barriers to engagement. This includes measuring improvements over time in response capabilities as a result of repeated drills and testing—highlighting a feedback loop for continuous improvement.

Operational response metrics such as emergency response times, availability of personnel, and information bottlenecks are also recommended as key KPIs. The lack of KPI training and measurement protocols in current emergency management training programs is flagged as a gap. Participants note that existing systems often can collect this data, but there is a missing layer of performance management tailored to emergencies. KPIs should not be nebulous, but instead be clear, concise, and ideally actionable. KPIs are needed to support justification for investments in city systems. Suggested metrics and approaches included:

- Calculating the percentage of the population practicing evacuation plans and determining how other plans interact within designated regions, districts, and neighborhoods.
- Assessing the propensity for households to practice, prepare for, and drill for hazard incidents. Response times, awareness of evacuation routes and effective execution could potentially be based on simulations and community exercises.
- Measuring how the community manages digital poverty and provides knowledge of how to gain access to emergency instructions and use and understand digital warning systems.
- Testing of emergency Standard Operating Procedures through public access to determine both breadth of accessibility and clarity of public instructions.
- Adopting existing standards (e.g., ISO 37123 and 37010) within a community to guide measurement of engagement and planned outcomes.

Protocols and methods should be developed to allow real-time measurement of community sentiment and awareness using hyperlocal data around resilience within (e.g.) different housing districts, flood zones, or school districts to measure how aware people are of the data that overlaps them. Exercises and simulations using realistic scenarios that illustrate measurable impacts could be used to collect data that reflects both local and expert knowledge.

Finally, the conversation touched on the value of international standards, particularly ISO standards for smart cities, which can offer a flexible framework for cities to contextualize resilience and preparedness metrics. The group also emphasized the importance of measuring at multiple levels—individual, household, neighborhood, city, and region—and across all disaster phases: mitigation, preparedness, response, and recovery. Together, these ideas advocate for a multi-scale, people-centered approach to measurement.

Summary Points from Question #3:
What Key Performance Indicators (KPIs) should be developed and integrated into a community information sharing and decision support system for disaster preparedness and recovery?
(i.e., What do we measure, and How do we measure it?)

- **Assessed knowledge held by the population based on percentage of population practicing evacuation plans and interacting with decision-makers within designated regions, districts, and neighborhoods.**
- **KPIs based on propensity for households to practice, prepare, drill for hazard incidents. Response time and awareness of evacuation and effective execution based on simulations and actual exercises.**
- **KPIs should measure not only overall system performance but also the distribution of outcomes across different neighborhoods and demographics (diversity and equanimity in evaluating outcomes).**
- **How the community manages digital deserts and provides knowledge of emergency instructions and warning systems for underserved communities.**
- **Testing of emergency Standard Operating Procedures through public access to determine both breadth of accessibility and clarity of public instructions.**
- **Community adoption of existing standards (e.g., ANSI/ISO 37123, 37010) within a community to guide measurement of engagement and planned outcomes.**

5.4 Question #4

How should operational considerations—i.e., efficiency of command/control/coordination—be balanced with civic considerations such as transparency/access/equity and the maintenance of public trust?

This conversation centered on how to balance operational efficiency—such as command, control, and coordination—with civic values like transparency, access, equity, and public trust. There was a strong consensus across groups that transparency and trust must be foundational. Participants emphasized the need for regional collaboration, particularly among city councils, to overcome institutional silos and improve emergency management. This includes top-down leadership and policies that enforce cross-jurisdictional cooperation. Considerations of the balance between transparency and expediency should also take into account the scale and type of disaster or crisis, immediate effects and existing hazards, and the effects on the population and urgency of response and recovery. In particular, restoration of critical public services such as water and electrical power, and recovery of communications, transportation and logistics networks may take priority during the initial phases of recovery of city services.

Building public trust emerged as a critical theme. One group highlighted the importance of consistent, small, value-driven actions and the need for community members who can "cross-pollinate" ideas across groups. They advocated for using plain, accessible language in public communications and emphasized community empowerment through genuine engagement and responsive leadership. Japan's approach to emergency management was cited as a model, particularly its inclusive and multilingual "Welcome App" for public awareness. Establishment of community working groups and organizations, whether prior to or during an incident can serve to empower the affected population in joint recovery efforts and community liaison.

Data privacy was also a concern. Participants noted the ethical implications of using personal data during emergencies and recommended re-establishing consent even in urgent situations. They stressed the importance of classifying, managing, and educating the public about open data to promote equitable access and responsible use. Cities, they argued, must take responsibility for helping residents understand and benefit from available data. Enabling the redirection of some "protected" data to limited or controlled accessibility during a crisis may serve to engage the public constructively while mitigating fear of widespread data sharing or misappropriation. The participation of trusted leaders and non-profits such as National Voluntary Organizations Active in Disasters (VOADs) can establish intermediaries between crisis decision makers and the affected population and assist in maintaining public trust.

Finally, the discussion highlighted the need to center community voices, especially in historically underserved areas. Successful engagement required involving trusted local figures like ministers and community center staff in outreach efforts. By ensuring those with lived experience are actively involved, governments can craft strategies that are both culturally responsive and trusted by the communities they aim to serve.

Summary Points from Question #4:
How should operational considerations—i.e., efficiency of command/control/coordination—be balanced with civic considerations such as transparency/access/equity and the maintenance of public trust?

- **Strong consensus that transparency and trust must be foundational both for equity in community engagement and for operational effectiveness and success in achieving sustainable resilience.**
- **Need for regional collaboration, particularly among city councils, to overcome institutional silos and improve crisis management with leadership and policies that enforce cross-jurisdictional cooperation**
- **Dedicated outreach to ensure public awareness that restoration of critical public services (water; electrical power; communications and transportation networks) takes priority during initial recovery**
- **Use of plain, accessible language in public communications (not agency jargon) with emphasis on community empowerment through genuine engagement and responsive leadership.**
- **Educating the public about open data to promote equitable access and responsible use, with cities taking responsibility for helping residents understand and benefit from available data**
- **Centering community voices, especially in historically underserved areas, ensuring those with lived experience are actively involved in building trust between government and the communities they serve.**

6. A Research Agenda for Whole Community Preparedness

During the third workshop held at the 2025 Natural Hazards Workshop in Boulder, Colorado, a fifth question was added specifically directed at defining a research agenda for future work: *"What research questions need to be addressed as a basis for an empirically grounded approach to community preparedness in Smart Cities?"* Two specific areas of investigation stood out:

(1) Research into the adoption or employment of Artificial Intelligence in disaster management and public collaboration in such a way that AI-generated outcomes of emergency- and crisis-related decisions are trustworthy and viewed by the public as serving the community's interest and safety.

(2) Research into the potential for online digital games to enhance planning through simulation, and thereby increase public adoption of disaster preparedness measures, particularly by engaging with and educating students and the younger generation of community residents (and potentially their parents).

In combination with the integration of these two capabilities into high-fidelity digital twins for a specific region or community, there is great potential for AI-based decision-making and the use of online games to prepare the public in a more engaging and accessible manner than the current practice of sparsely attended table-top exercises and preparedness pamphlets and public service websites.

Looking ahead, a number of key areas emerged from the workshop discussions as priorities for future action. To build a resilient whole community approach, NIST and its partners should focus on developing standards, strengthening public-private partnerships, and creating pilot programs that test innovative solutions for disaster preparedness and response. These initiatives would support the development of interoperable systems, resilient infrastructures, and community-centered engagement strategies, forming a foundation for more robust preparedness efforts.

> **Pilot Platforms as Test Beds:** Participants supported the idea of pilot platforms or test beds that could model effective, scalable resilience solutions. "A test bed under NIST's guidance would allow us to experiment with new ideas safely and refine them before rolling them out on a larger scale," an attendee noted.

- **Develop standards and protocols for emergency communications in the civil sector.** Convening key public and private stakeholders to work on basic data exchange and interoperability standards will enable faster, more effective coordination across agencies and sectors. Standardizing these protocols can facilitate immediate data-sharing, ensuring that emergency management and response teams have real-time access to critical information. Where feasible, coordinating these efforts with current international standards organizations (notably ISO, IEC and IEEE) would potentially increase the credibility and ease of adoption by many communities—particularly larger metropolitan cities.

- **Consider Pilot Projects to Apply Standards in Real-World Settings**: Implementing pilot projects, particularly in high-risk areas, can provide valuable insights into how standardized communication and operational protocols function in practice. These pilots would test interoperability and improve communication efficiency, especially in communities where streamlined response is most essential.

> **Pilot Programs as Catalysts for Innovation:** Participants saw pilot projects as a way to champion innovative resilience solutions and demonstrate effective models. "NIST's advocacy and influence can drive pilot projects forward, offering real-world proof of concept and inspiring broader adoption," one attendee observed.

- **Build or Strengthen Public-Private Partnerships**: Engaging telecommunications providers, technology companies, and community organizations to establish a coalition focused on resilient communication infrastructure will enhance resource-sharing and operational support. Formalized partnerships with private sector entities will ensure access to essential services during emergencies, particularly in telecommunications and logistics.
- **Develop Model Memoranda of Understanding (MOUs) with Private Sector Partners**: To ensure rapid access to resources and services, model MOUs should be developed, outlining responsibilities and expectations for private partners during disasters. These agreements would clarify roles in crisis scenarios, enabling smoother, faster collaboration between public and private sectors within affected communities, cities, and regions.

> **Aligning Visions Through a Model Framework:** Participants discussed how a NIST model framework could serve as a unifying guide for aligning the visions and missions of diverse agencies and sectors. "NIST's framework could provide the structure we need to bring different entities together under a common objective, ensuring all stakeholders are on the same page," noted one attendee, emphasizing that such a model would help address obstacles like siloed thinking and inconsistencies across agencies.

- **Launch Pilot Programs within Resilience Centers**: Establishing pilot resilience centers in selected communities could serve as operational hubs for both everyday services and emergency response. These centers would support ongoing community engagement, training, and education on disaster preparedness, while also offering a valuable data source for studying public engagement and response behaviors. Priority should be given to developing and implementing dual-use technologies that can function during both normal community routine and also during crisis situations (i.e., "Blue-Sky" and "Gray-Sky" conditions).

- **Enhance Community Engagement Strategies**: Developing culturally appropriate messaging toolkits and disseminating trusted information through channels like local leaders, churches, and cultural organizations will strengthen community resilience. Two-way communication platforms can also be implemented to allow residents to ask questions, give feedback, and report issues in real time during emergencies.
- **Conduct Scaled Emergency Exercises**: Organizing tabletop and scenario-based exercises that include public, private, and nonprofit sectors will help refine response protocols. By starting with smaller exercises and progressively involving larger communities, these simulations can help scale and improve the whole community approach, addressing both technical and social aspects of preparedness. Exercises should focus on exploring techniques for effective community collaboration and should be carried through the response phase and include participation by private sector and economic development enterprises, as well as by local non-profits (e.g., faith-based organizations, schools, and civic organizations).

Collaborating with DHS for Modeling Response and Governance Structures: Attendees discussed the potential for NIST to partner with DHS on pilot programs aimed at building model governance structures for disaster response and recovery, and critical infrastructure frameworks for interoperability. "If NIST and DHS can develop a standard through these pilots, it would provide a powerful example of integrated governance in local emergency situations and crises for communities nationwide," one participant commented.

Summary Findings from the workshop series

In light of these themes explored through the workshop series, the following items are recommended as next steps for a research agenda to further define requirements, priorities, and resources toward developing a national Whole Community strategy that could be capably executed by state and local authorities:

(1) Develop protocols and standards for public safety communications for the civil sector and test those standards in real-world settings;
(2) Define approaches for strengthening public-private partnerships across communities;
(3) Develop model Memoranda of Understanding (MOUs) for formalizing community collaboration among private sector partners;
(4) Initiate a pilot program to develop community resilience centers and engagement strategies;
(5) Conduct scaled emergency exercises that include the recovery phase of the disaster cycle to validate strategies for community recovery and restoration of infrastructure, economic stability, and social and cultural cohesion; and

(6) Define measures and metrics for analyzing and evaluating competing approaches of governance, collaboration and coordination of post-disaster recovery.

The box below summarizes what were the most commonly cited findings of the Workshop series, and offers priorities and a starting point for future research and development for achieving a true strategy for Whole Community Preparedness.

Summary outcomes from the Whole Community Preparedness Workshop Series

- **Build a publicly accessible, dual-use communications system for information sharing to enable community collaboration, planning, and coordination during civil emergencies**
- **Establish community and neighborhood Resilience Centers for local coordination and mobilization of resources**
- **Develop standard communication and operational protocols common across regions**
- **Research, develop and enhance community engagement strategies**
- **Conduct pilot projects to apply and test protocols/standards in real-world settings**
- **Build and strengthen Public-Private Partnerships through community engagement with emphasis on identifying and leveraging private sector resources**
- **Conduct scaled emergency exercises that involve elected officials, community leaders, and private sector organizations and extend through the Recovery Phase.**

Appendix A. Charter Document and Read-Ahead for Workshop Participants

This appendix provides the guiding documents that framed the approach adopted during the initial workshop conducted in August 2024 and was distributed to attendees prior to the workshop to provide additional background and a series of research questions that served as the foundation for presentations and discussions during the workshop. The questions used during the first workshop were modified slightly and used to frame discussions and research questions during the second workshop of city administrators and elected officials conducted in April 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Workshop on Whole Community Preparedness in Smart Cities and Communities

BACKGROUND

The Smart City Infrastructure program of the National Institute of Standards and Technology (NIST) leads a national public-private partnership of cities, private sector organizations and research centers committed to improving city services and operations and residents' overall quality of life through the integration of advanced digital technologies. An important dimension of the Smart City program is developing concepts, technologies, and standards for improving public safety, health, and disaster resilience for all communities.

In 2011, the Federal Emergency Management Agency (FEMA) initiated the "whole community" approach to disaster management with the goal of engaging community stakeholders—to include private sector entities, local agencies, and civil society—in building disaster resilient communities. In 2013, the Centers for Disease Control and Prevention (CDC) adopted a similar concept for public health. However, the COVID-19 crisis revealed fundamental challenges in implementing a national strategy in individual cities and communities. Difficulties in local execution of the strategy provided evidence that implementation of a national "whole community" approach will require significant research, investment, public engagement, and a standardized organizational structure and communications infrastructure.

PROJECT OVERVIEW

To address this challenge, NIST is launching a research project to define technology applications, analyses, key performance indicators, and adaptive decision architectures for public safety planning for Smart Cities and Communities. The project will develop an AI-enhanced information-sharing and analysis capability to enable collaborative decision-making between civil authorities, emergency managers, and a community's population., This multi-agency, cross-disciplinary capability will allow communities, cities, and regions to respond to and recover from large-scale disasters and emergencies more effectively, and support scenario-based exercises to evaluate alternate approaches to managing large-scale hazards and disaster impacts.

PROJECT OBJECTIVES

The goal of this research project is to define a structure for improving community safety, security, economic vitality, and overall community resilience through integration of advanced technologies into city operations and infrastructure. Key to this approach is the inclusion of the resources, capabilities and talent resident in the community, its population, and the private sector. Outputs from the workshop will help establish the technical and operational foundation for a true “whole community approach” to disaster preparedness and resilience. The resulting system will be piloted in select smart cities and communities and adopted as a foundation for public safety within the NIST Smart Cities Infrastructure program.

THE WORKSHOP

To initiate this effort, the Smart City Infrastructure program will host a technical workshop to explore the concept and preliminary design for a technology application—a cyber-physical-social system—directed at enhancing public safety, health, and community resilience for Smart Cities and Communities. The workshop will bring together a team of senior first responders, emergency managers, and city, state, and federal authorities to provide perspective on current and future requirements for enabling communities to more capably manage complex threats to public safety, health, and community welfare. Workshop participants will help NIST define the acceptability, feasibility, and general structure of an integrated communications infrastructure to support community disaster planning and response and improve multi-agency crisis communications among local officials and leaders to more effectively manage complex crises. General workshop objectives include

- Defining an integrated communications infrastructure to enhance collaborative decision-making and support a "whole community approach" to public safety during national-scale emergencies.
- Framing a standard approach for smart city disaster recovery, leveraging state-of-the-art technologies to enhance coordination between federal, state, and local agencies and civil authorities.
- Identifying requirements for an information-sharing and analysis capability to enable collaborative decision-making among civil authorities, community leaders, and the local population.

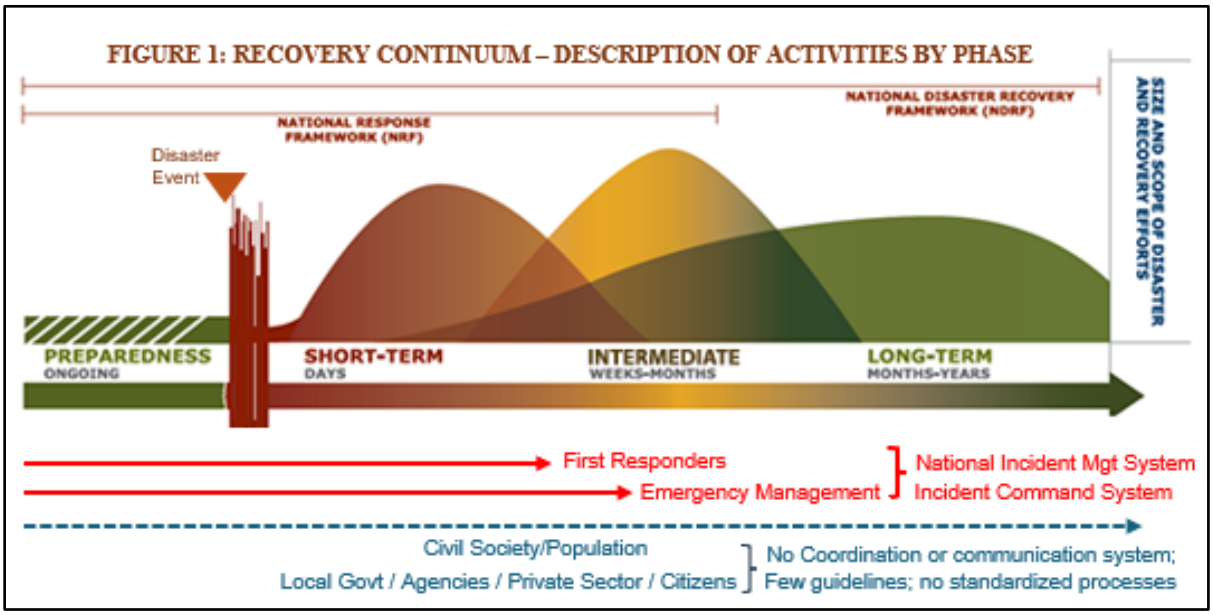

Fig. 1. Recovery Continuum defined in the National Disaster Recovery Framework and the challenge for local authorities and the affected population

Figure 1 from the National Disaster Recovery Framework (NDRF) illustrates the gap in coordination and communications infrastructure that this workshop will address. As the red vectors below the NDRF Recovery Continuum illustrate, first responders and emergency managers operate within the organizational structure, doctrine, and dedicated communications networks defined by the National Incident Management System and Incident Command System. In contrast, local authorities, and the civil sector (the dotted blue vector) have no dedicated organizational framework, operational protocols, standards, or communications channels for coordination of long-term disaster recovery. Consequently, there is no formal structure for comprehensive situational awareness and coordination between response agencies and the community as a whole.

This workshop will initiate a NIST research effort to define the acceptability, feasibility, and general structure of an integrated communications infrastructure to support community disaster planning and response and improve multi-agency crisis communications among local officials and leaders to more effectively manage complex crises.

The workshop has been designed to bring together as wide a spectrum of expertise as possible in a short (two-day) event. Attendees from the following sectors will be represented.

- Federal Agencies (NIST, DHS, FEMA, CISA, DOS)
- State/Local Government and Emergency Management
- Federal Research Laboratory / FFRDC
- Industry and Business Sector
- Research Universities and Non-Profits

QUESTIONS TO FRAME THE WORKSHOP DISCUSSIONS

In preparation for the workshop, we ask you to consider the following questions as a framework for the discussions that will take place in the plenary and break-out sessions.

1. How might an integrated communications infrastructure enhance collaborative decision-making for planning, response, and recovery supporting a "whole community approach" to public health and safety as a mitigation strategy against national-scale civil emergencies?
    a. What aspects of an integrated communications infrastructure should be developed to properly support local communities?
    b. How can decision-making technology help federal, state, and regional disaster management provide support that is attuned to community needs and capabilities?
    c. What other considerations should the workshop consider in order to properly develop an approach to an integrated communication infrastructure?
2. Should a community decision support system available to elected officials and civic leadership be:
    a. Fully integrated with Emergency Management (e.g., via an EOC web-based dashboard)?
    b. Stand-alone and isolated/firewalled from Emergency Management decision systems and public safety communications?
    c. Accessible to Emergency Management for situational awareness, but not accessible to the civil sector and general public?
3. Should a community-focused decision support system be designed as
    a. A dual-use system (i.e., functional on both Blue-Sky (normal) and Gray-Sky (crisis) days)?
    b. Or as a dedicated system to be reserved for local/civic preparedness, response, recovery only (i.e., a dedicated system rather than a dual-use system)?
    c. If functional for both Blue- and Gray-Sky days, how should the transition between such functions be implemented, and who should control implementation of the transition?
4. If a community-focused decision support system were designed as a dual-use system (i.e., functional for both Blue- and Gray-Sky days) what Blue-Sky functions should it incorporate? For example,
    a. Monitoring and measurement of natural environmental conditions
    b. Critical infrastructure sensing and monitoring in real-time

   c. City and urban planning; alternative design modeling, economic planning and analysis
   d. Public information-sharing (e.g., a city dashboard) with access to traffic cameras and public space or street views
   e. Other functions?

5. What Key Performance Indicators (KPIs) should be prioritized for development and integration into a community decision support system? (Consider KPIs that reflect operational, economic, social, or environmental dimensions of city operations and functions).
6. Within a community-focused decision support system, how should operational considerations (efficiency of command/control/coordination) be balanced with public considerations such as transparency/access/equity, and the maintenance of public trust?
7. What other questions not listed here should be considered for discussion? Consider this question from the perspective of support to and by your own agency, organization, or sector.

Appendix B. Workshop Agenda

Workshop on Whole Community Preparedness in Smart Cities and Communities

The George H.W. Bush School of Government and Public Service, Washington, D.C.

B.1. Agenda Day 1

Time	Purpose	Presenter
8:00 AM	**Registration**	Energetics
9:00 AM	**Welcome and Administrative Notes**	NIST, Texas A&M Univ., Energetics
9:10 AM	**Welcoming Remarks from Host** Bush School of Government and Public Service	Lt. Gen. (Ret.) Jay B. Silveria, Executive Director
9:15 AM	**Introduction to NIST and Workshop Origins** Day 1 Focus: Foundational aspects of a "Whole Community Approach" to national preparedness	Michael Dunaway, Smart Connected Systems Division, NIST
9:30 AM	**Day 1 Keynote Address** *Q/A to follow*	Sec. Russell Strickland, Maryland Department of Emergency Management
10:15 AM	**Federal Agency Panel –** Perspectives on an integrated Whole Community Approach to national preparedness *Q/A to follow*	Zach Smith, FEMA Jeffrey Booth, DHS David Nolan, CISA
11:10 AM	**Breakout Session Logistics**	Energetics
11:15 AM	**BREAK** *Attendees move to Breakout Rooms*	*Breakout Rooms A, B, C, D*
11:30 AM	**Breakout Session 1 –** What ***foundational aspects*** (e.g., technical, social, cultural) are essential to support a Whole Community Approach to disaster preparedness, response, and recovery?	*Breakout Rooms A, B, C, D*
12:30 PM	**LUNCH (on your own)**	
1:45 PM	**Report Out from Breakout Session 1**	Energetics
2:30 PM	**Breakout Session 2 –** What are ***technical and operational elements*** of an integrated communications infrastructure that would support whole community preparedness and resilience?	*Breakout Rooms A, B, C, D*
3:45 PM	**BREAK**	
4:00 PM	**Report Out from Breakout Session 2**	Energetics
4:45 PM	**Day 1 Summary and Next Steps for Day 2**	Energetics. NIST
5:00 PM	**Adjourn for Day 1**	

B.2. Agenda Day 2

Time	Purpose	Presenter
8:00 AM	**Registration**	Energetics
9:00 AM	**Welcome and Administrative Notes**	Energetics
9:10 AM	**Day 2 Focus** Implementing an integrated "Whole Community Approach" to national preparedness	Michael Dunaway, Smart Connected Systems Division, NIST
9:15 AM	**Day 2 Keynote Address** *Q/A to follow*	Dr. James Kendra, Director, Disaster Research Center, University of Delaware
10:00 AM	**CISA Connected Communities Initiative**	Laura Hershon, Branch Chief, CISA CCI
10:45 AM	**Breakout Logistics**	Energetics
10:55 AM	**BREAK**	
11:00 AM	**Breakout Session 3 –** What are the ***requirements and conditions for implementing*** a Whole Community Approach for national preparedness and resilience? What are the technologies, infrastructures, doctrines, and strategies to do so?	*Breakout Rooms A, B, C, D*
12:00 PM	**LUNCH (on your own)**	
1:15 PM	**Report Out from Breakout Session 3**	Energetics
2:00 PM	**Use of a Digital Twin for City Operations and Community Preparedness**	Marc Stolzenberg, Emergency Manager, and Raimundo Rodulfo, CIO, City of Coral Gables, FL
2:45 PM	**BREAK**	
3:00 PM	**Group Discussion –** What ***strategies*** should be pursued to establish a Whole Community Approach to national preparedness and resilience? What role could IT and other technologies play in that strategy?	Energetics
4:00 PM	**Summary Comments and Next Steps**	Energetics, NIST
4:30 PM	**Adjourn**	

Appendix C. Presentation and Panel Summaries

C.1. Day 1 Sessions and Presentations

Keynote Address: State of Emergency Management

Russel Strickland, Secretary of the Maryland Department of Emergency Management

To kick off the workshop, Secretary Russell Strickland, Maryland Department of Emergency Management delivered a keynote address discussing the challenges, opportunities, and evolving nature of emergency management. Strickland, who has over 40 years of experience in emergency management and civil service, was reappointed in 2023, reflected on the shifting responsibilities of emergency services since the 2003 Homeland Security Act. He emphasized how the definition of "all hazards" has grown to include school violence, the opioid epidemic, cybersecurity, and food resilience. In particular, the COVID-19 pandemic highlighted the vulnerabilities in the food supply chain, prompting Maryland to establish a Food Resilience Council. Strickland also underscored the importance of "left of boom" preparedness—mitigating risks before disasters strike—which helps lower the costs of response and recovery.

He highlighted the increasing frequency and severity of disasters due to climate change, such as wildfires, floods, and hurricanes, and stressed that government alone cannot manage these challenges without private sector collaboration. Strickland noted that although Maryland is a relatively safe state with fewer federally declared disasters compared to others, the state has experienced a surge in disaster declarations in the last two decades. He promoted Maryland as a good location for businesses due to its lower disaster risk but acknowledged the rising pressure on emergency management to adapt.

Strickland emphasized the need for new tools and technologies, especially AI, to help emergency management agencies respond more efficiently. He discussed Maryland's collaboration with FEMA and other agencies to use systems like the Community Lifeline Status System for better disaster coordination. The state also set up a Risk Analysis Unit to predict and prepare for potential risks. Artificial Intelligence (AI) is already being used for tasks like drafting plans and press releases, and it could eventually help reduce workforce shortages in emergency management by automating some tasks.

During the Q&A session, Strickland addressed questions about the role of AI in consolidating information during emergencies and the need for clear communication with the public to foster trust in AI. He also discussed the importance of community relationships in recovery efforts and managing change when new technologies are introduced, especially in fast-paced emergency environments where personnel may require immediate training. Strickland concluded by emphasizing that, while technology is critical, human oversight and a compassionate, data-driven approach must always guide emergency management efforts.

C.2. Federal Agency Panel

Zach Smith
Emergency Management Specialist, Federal Emergency Management Agency (FEMA)

Jeffrey Booth
Director, Sensor and Platform Technology Center, Science and Technology Directorate, US Department of Homeland Security (DHS)

David Nolan
Emerging and Advanced Technology Branch Chief, Emergency Communications Division, Cybersecurity and Infrastructure Security Agency (CISA)

The Federal Agency Panel, featuring Zach Smith (FEMA), Jeffrey Booth (DHS) and David Nolan (CISA), provided perspectives on an integrated whole community approach to national preparedness from the perspective of federal agencies with responsibilities for public safety. Speakers discussed key initiatives, emerging technologies, and challenges in emergency management.

Zach Smith introduced FEMA's Strategic Foresight Initiative 2050 (SFI 2050), which aims to prepare the emergency management community for unprecedented changes and uncertainties in the future. This initiative involves a multi-phase process—framing, scanning, forecasting, workshopping, and reporting—designed to explore possible futures and develop long-term strategies. Workshops have been conducted with participants from various sectors to simulate responses to different future scenarios. The final report will guide FEMA's 2026-2030 Strategic Plan.

David Nolan from CISA's Emergency Communications Division focused on emergency communications and the importance of interoperability, especially in the context of smart cities and emerging technologies. His team works on ensuring that public safety communications systems are secure and resilient. He highlighted CISA's three-layer information-sharing architecture, which collects and organizes data from Internet of Things (IoT)-based devices and other sources to provide real-time information to responders. Nolan also shared a Public Safety Communications and Cyber Resiliency Toolkit available to the public, which includes resources for emergency infrastructure.

Jeffrey Booth discussed DHS Science and Technology Directorate's efforts to deploy "left-of-boom" technologies, which aim to prevent disasters before they escalate. For example, DHS has deployed wildfire and flood sensors in various locations to detect early warning signs. These sensors have proven effective in reducing the need for swift water rescues and providing early wildfire detection. Booth emphasized the need for a holistic approach that involves collaboration between government, private sector, and local communities to ensure that advanced technologies are successfully adopted and commercialized, avoiding the "valley of death" where promising technologies fail due to lack of support.

During the Q&A, panelists addressed gaps in community resilience and the need for improved standards and protocols. Smith pointed out that risks are increasingly interconnected, such as cyberattacks on critical infrastructure impacting local areas. Social disconnection is another growing concern, as strong community ties are vital for resilience, yet social isolation is on the rise. Booth and Nolan discussed the role of emerging technologies, like AI and sensors, in enhancing disaster preparedness and recovery, stressing the importance of interoperability and privacy concerns. Open-source software was also highlighted as a crucial tool for smaller jurisdictions that may lack the resources to invest in proprietary systems. Finally, the panelists emphasized the importance of pre-boom preparedness and education, urging communities to familiarize themselves with available technologies and resources before disasters strike.

C.3. Day 2 Sessions and Presentations

Keynote Address: Resilience, Social Capital, and Emergent Behavior

James Kendra, Director of the Disaster Research Center (DRC) at the University of Delaware

In the second day of the workshop, Dr. James Kendra, Director of the Disaster Research Center (DRC) at the University of Delaware, gave a keynote address on the role of resilience, social capital, and emergent behavior in disaster recovery. Dr. Kendra framed resilience as not just the ability to "bounce back" from disasters but also to "bounce forward," meaning that communities can recover and thrive despite the challenges they face. While no single definition of resilience is universally accepted, the general consensus involves communities recovering quickly, surviving, and even thriving after disasters. Kendra cited key scholars, including Aaron Wildavsky and David Alexander, and emphasized that resilience is deeply rooted in social networks, emergent behavior, and the ability of communities to act creatively in crisis situations.

A case study on the maritime evacuation of Manhattan during 9/11 highlighted the critical role of emergent, spontaneous behavior in disaster situations. Between 300,000 and 500,000 people were evacuated by an uncoordinated flotilla of tugboats, private yachts, and other vessels. This unplanned effort demonstrated how social capital, local knowledge, and informal networks can enable communities to respond effectively in the absence of official direction. The operation's success underscored the importance of community ties and the flexibility of individuals in crisis. Kendra highlighted how local boat operators, despite being competitors, acted collectively, driven by a sense of duty, to evacuate people from Lower Manhattan, demonstrating the latent disaster response capabilities within communities.

Dr. Kendra explored whether social capital could be operationalized, discussing a project with Johns Hopkins University called Composite of Post-Event Well-Being (COPEWELL), which was funded by the CDC to systematically assess community resilience. The project moved away from creating a simple "Community Resilience Index" score and focused instead on understanding the dynamic nature of resilience over time. The system dynamics model developed in this project combined various factors like education, healthcare, transportation, and social cohesion to predict a community's ability to recover after a disaster. While conceptual models proved useful in visualizing these relationships, Kendra noted the challenges of obtaining data that adequately reflects social capital elements, such as local partnerships or community trust.

Kendra concluded by emphasizing the need for both technological tools and strong social foundations in disaster management. Drawing a parallel to the Churchill War Rooms during World War II, he pointed out that, despite advancements in technology, the core challenge remains how to use tools effectively without losing the human element. Social capital, emergent groups, and the relationships between community members are at the heart of resilience, and they continue to be vital in ensuring communities can face and recover from disasters.

C.4 CISA Connected Communities Initiative

Laura Hershon, Branch Chief, Connected Communities Initiative, Cybersecurity and Infrastructure Security Agency (CISA)

Laura Hershon, Branch Chief of the Connected Communities Initiative (CCI) within the Cybersecurity and Infrastructure Security Agency (CISA), showcased CCI's aims in providing municipalities with best practices and mitigation strategies for smart city technologies by conducting cyber and physical risk analyses and collaborating with local leaders. CCI's mission is to help municipal leaders deploy resilient technology while addressing the risks that come with expanding their technological infrastructures. With the increased adoption of smart technology, cities face a broader attack surface, and the initiative seeks to mitigate these vulnerabilities by offering products, resources, and guidance that are accessible even to those without a technical background. CISA emphasizes the importance of a bidirectional feedback loop with stakeholders to ensure that analysis and recommendations align with the needs of connected communities.

CISA focuses on small and medium-sized municipalities, which it describes as "target rich, resource poor" (TRRP), meaning they have a significant amount of technology but limited resources to secure it. The Cybersecurity Best Practices for Smart Cities Guide, developed in collaboration with the FBI, NSA, and international partners, addresses three primary areas of risk: the expanded attack surface from interconnected systems, supply chain risks from vendors with weak security practices, and the operational risks of automated systems. The guide promotes proactive supply chain risk management, secure system design from the start, and operational resilience through staff training and manual system operations. CISA's "Secure by Design" approach pushes vendors to deliver products that are secure when sold, rather than relying on patches after vulnerabilities are discovered.

An Internet of Things (IoT) risk assessment examines the risks associated with IoT devices, breaking them down into three layers: perception, transport, and application. Each layer poses distinct risks, from unprotected devices and sensors to data vulnerabilities during transmission and processing. IoT devices can affect citizens directly, especially in areas like utilities or transportation, and failures in these systems can erode trust in public services. Mitigating these risks involves maintaining an inventory of IoT devices, encrypting data, and asking vendors key questions during procurement. Hershon also stressed the importance of staff training to manage and mitigate IoT-related risks effectively.

During the Q&A session, Hershon addressed concerns about ensuring that products are secure by design, even for municipalities with limited resources. CISA is working on simplifying guidelines and frameworks so that smaller municipalities can easily ask the right questions of vendors. Although there are no formal requirements for secure-by-design products, CISA is pushing for voluntary adoption and encouraging municipalities to use their purchasing power to demand security assurances. Hershon also discussed CISA's capacity for security analytics and red teaming, acknowledging the limitations of their resources but offering guidance for municipalities seeking external vendors. Additionally, partnerships with universities and cybersecurity programs were proposed as a way to involve students in helping municipalities assess and enhance their cybersecurity measures.

C.5. Use of a Digital Twin for City Operations and Community Preparedness

Marc Stolzenberg, Emergency Manager, City of Coral Gables, Florida
Raimundo Rodulfo, Chief Innovation Officer, City of Coral Gables, Florida

From the City of Coral Gables, Florida, Marc Stolzenberg, Emergency Manager, and Raimundo Rodulfo, CIO, presented the innovative use of a digital twin to enhance city operations and community preparedness, with a focus on disaster resilience. The city has developed a technological and operational foundation that integrates smart city infrastructure to create a comprehensive whole-community approach to disaster preparedness. This approach builds on lessons learned from previous incidents, such as their response to Hurricane Irma in 2017 and the COVID-19 pandemic, to continually improve their response strategies and enhance community trust and engagement.

The city's Digital Twin serves as a real-time, live model of Coral Gables, created with advanced photogrammetry and Building Information Modeling (BIM). It allows city officials, first responders, and emergency managers to simulate both natural and man-made disasters, aiding in tactical decision-making. For example, simulations can forecast the effects of hurricanes or manage city events like the World Cup, ensuring preparedness for large gatherings. Drones and floating water sensors are deployed for tasks such as site inspections, surveillance, and emergency response, with the drone fleet capable of reaching any part of the city in under 3 minutes.

The city's resilience infrastructure is built on fiber optics, with multiple layers of redundancy, including Gigabit wireless networks, Metropolitan Ethernet, cellular, and satellite systems. This robust network ensured operational continuity during Hurricane Irma and remains a critical component of Coral Gables' disaster response strategy. The city's smart technology ecosystem integrates IoT sensors for monitoring traffic, environmental conditions, and public safety. These sensors provide hyperlocal data, processed with AI to enhance situational awareness and decision-making during emergencies.

Stolzenberg and Rodulfo also emphasized community engagement through programs like Neighborhood Ambassadors and the Senior Advisory Board, who help communicate with vulnerable populations during disasters. Coral Gables has invested in social equity and active communication, ensuring residents, especially seniors, receive clear and accessible information. The Smart City Hub Platform, developed in-house, enables real-time data access for residents. Additionally, the city fosters innovation through internship programs and the development of a metaverse model, taking the next step in virtual engagement for emergency planning and infrastructure management.

Appendix D. References and Resources

The following section provides selected bibliographic references and links to documents cited in this report along with additional resources relevant to smart cities and communities.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

_____ Smart Cities and Communities: A Key Performance Indicators Framework. NIST Special Publication 1900-206. Feb 2022. https://www.nist.gov/publications/smart-cities-and-communities-key-performance-indicators-framework.

_____ Global Community Technology Challenge (GCTC) Strategic 12 Plan 2024-2026. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 13 (SP) NIST SP 1900-207. https://doi.org/10.6028/NIST.SP.1900-207.

_____ Blueprint for Smart Public Safety in Connected Communities. Global City Teams Challenge. Aug 2017. Blueprint for Smart Public Safety in Connected Communities - OpenCommons

_____ Artificial Intelligence Risk Management Framework (AI RMF 1.0) NIST AI 100-1. Jan 2023. https://doi.org/10.6028/NIST.AI.100-1

_____ NIST Cybersecurity Framework (CSF 2.0). Feb 2024. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

_____ National Response Framework. / National Incident Management System. Washington, D.C. 28 Oct 2019. https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response.

_____ National Disaster Recovery Framework and Recovery Support Functions. Washington, D.C. June 2016. https://www.fema.gov/national-disaster-recovery-framework; https://www.fema.gov/recovery-support-functions.

_____ A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action. FDOC 104-008-1 Dec 2011. https://www.fema.gov/sites/default/files/2020-07/whole_community_dec2011__2.pdf.

_____ Pandemic Response to Coronavirus Disease 2019 (COVID-19: Initial Assessment Report. January 2021. Washington D.C. Accessed 28 Aug 2021. https://www.fema.gov/disaster/coronavirus/data-resources/initial-assessment-report.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

CISA Connected Communities. Webpage: Connected Communities | Cybersecurity and Infrastructure Security Agency CISA

Appendix E. Workshop Participants.

NIST acknowledges with gratitude the participation and contributions of the following individuals at the Workshops on Whole Community Preparedness.

August 2024 Workshop at George H.W. Bush School, Washington, D.C.		
Last Name	**First Name**	**Organization**
Alfonzo	Mariela	State of Place / New York University
Barbera	Joseph	George Washington University
Beam	Jonathan	US Ignite
Booth	Jeffrey	Department of Homeland Security
Carey	Christopher	Portland, Oregon Bureau of Emergency Management
Chelen	Julia	National Institute of Standards and Technology
Clavin	Christopher	National Institute of Standards and Technology
Collier	Chelsea	Digi.City
Cotter	Daniel	US Department of Homeland Security
Culhane	Craig	Sand Technologies
Dadja	Afeite	CTIA
Dean	Bradley	Council on Environmental Quality
Dulam	Rithika	National Institute of Standards and Technology
Eby	Charles	Maryland Department of Emergency Management
Green	Jacob	Mosslabs
Greenberg	Robert	G&H International Services, Inc.
Harrison	Ken	National Institute of Standards and Technology
Hershon	Laura	Cybersecurity and Infrastructure Security Agency
Horn	Andrew	Simsi, Inc.
Kahn	Alison	National Institute of Standards and Technology
Kendra	James	University of Delaware, Disaster Research Center
Lee	Derick	PilotCity Inc.
Lowry	Christian	Cybersecurity and Infrastructure Security Agency
Mahdavi	Mojdeh	US Ignite
Manuj	Ila	University of North Texas
Markhvida	Maria	New York University
Masuda	Michael	U.S. State Department
Neaves	Tonya	Global Connective Center
Nolan	David	Cybersecurity and Infrastructure Security Agency
O'Steen	Thomas	Sand Technologies
Poulin	Robert	Ogilvy
Pinfold	Wilfred	OpenCommons
Pravin	Dipakkumar	UNT-University of North Texas
Rodulfo	Raimundo	City of Coral Gables
Roth	Thomas	National Institute of Standards and Technology
Smith	Zachary	Federal Emergency Management Agency

Stolzenberg	Marc	Coral Gables Emergency Management
Strickland	Russell	Maryland Department of Emergency Management
Tandon	Arti	Smart City Expo USA
Tisdale	Rinda	National Institute of Standards and Technology
Treloar	Shandi	McChrystal Group
Wall	Kenneth	Office of NCR Coordination / FEMA / DHS
Waskom	James	WR Interests LLC
Wollman	David	National Institute of Standards and Technology

April 2025 Workshop at TechConnect Smart Cities Conference, San Antonion, TX and July 2025 Researchers Meeting, Natural Hazards Workshop, Boulder, CO

Last Name	First Name	Organization
Bargnesi	Leah	University at Buffalo
Brooks	Alison	IDC
Clavin	Chris	National Institute of Standards and Technology
Deacon	Aaron	KC Digital Drive
Deininger	Deborah	N5 Sensors
Enoch	Vanessa	Cultural Impact, LLC
Grigsby	Maleah	American Public Square
Gadhiraju	Vasu	Normal, Illinois
Hu	Allison	Circular San Antonio / HEB
Jenkins	Sean	Valgaska
Kaufman	Nick	inCitu, Inc.
Klingensmith	Chase	City of Pittsburgh, Pennsylvania
LaGrue	Kimberly	City of New Orleans, Louisiana
Lu	Pei-Jyun	Arizona State University
MacDiarmid	Alex	Quanterion Solutions
McPeake	Stephen	Civic Dollars
Nerurkar	Pamela	Texas A&M University
Nold	Kerstin	City of Chandler, Arizona
Pilisiwe	Masiba	Umzimuubu Municipality, South Africa
Pugh	Bill	True North Software Solutions
Sagert	Patricia	City of Maple Ridge, California
Schwartz	David	Rochester Institute of Technology
Scipione	Vincent	City of Syracuse, New York
Senthilkumar	Sanjana	Texas A&M University
Spikes	Eric	Sonda
Sumy	Danielle	National Science Foundation
Tamayo	Carlos	Phronimos, LLC
Tarin	Lauren	City of San Antonio, Texas
White	Rommia	Haven
Wong	Richard	Smart City CA USA

Yeganeh	Nasim	University of Florida	
Yesner	Ruthbea	IDC	

Workshop Coordination Team			
Dunaway	Michael	National Institute of Standards and Technology	
O'Fallon	Cheyney	National Institute of Standards and Technology	
Guo	Wenqi	National Institute of Standards and Technology	
Helgeson	Jennifer	National Institute of Standards and Technology	
Alfonzo	Mariela	State of Place / New York University	
Hu	Qian	George Mason University	
McCullough	Chelsea	Digi.City / Smart Cities Connect	
Pinfold	Wilfred	OpenCommons	
Rodulfo	Raimundo	City of Coral Gables, Florida	
Treloar	Shandi	McChrystal Group	
Alerion	Harper	Energetics	{Contract Support Personnel}
Giles	Lauren	Energetics	
Janocha	Kirstin	Energetics	
Qureshi	Mahia	Energetics	
Sigrist	Marc	Energetics	
Zalcman	Eric	Energetics	
Zalis	Walter	Energetics	