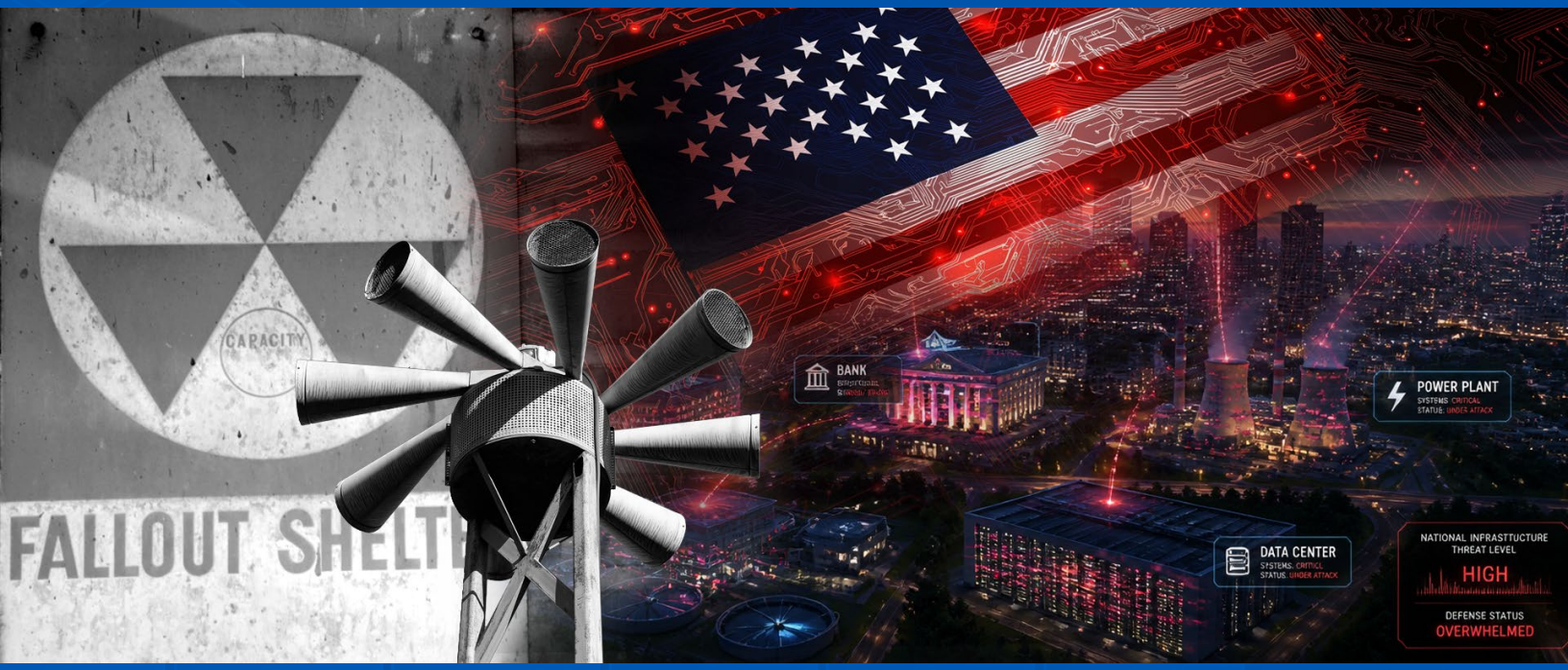
CNA

AUGUST 2026

Civil Defense in the 21st Century

Dawn Thomas, Carrie Shelton, Jamie Biglow, John Kearse, and Rachel Jones



IIM-2026-U-045818-Final

CNA

Abstract

This report examines the need for a renewed and revised approach to civil defense in response to an evolving threat landscape facing the United States. Current preparedness efforts address a range of hazards through an all-hazards framework but do not include distinct planning scenarios involving nation-state military attacks or coercion. The report examines historical civil defense efforts, current threats to the homeland, and gaps in civil defense planning. We developed a civil defense framework comprising three critical areas: providing population support and consequence management, protecting economic vitality and critical infrastructure, and maintaining public cohesion and will. The report focuses on population support and consequence management during complex incidents, including long-duration, widespread outages of critical infrastructure, and identifies challenges, potential consequences, and proposed solutions across 11 key areas of civil defense planning.

This work was internally funded by CNA.

Cover image: Jennifer Karras, CNA.

Approved by: **August 2026**

Dawn Thomas, Director
Center for Critical Incident Analysis, Safety and Security Division
Institute for Public Research

Request additional copies of this document through inquiries@cna.org.

Contents

This page intentionally left blank.

What Is Civil Defense?

Civil defense is defined as "the system of protective measures and emergency relief activities conducted by civilians in case of hostile attack, sabotage, or natural disaster."[1]

During the height of the Cold War era (spanning the late 1940s to the early 1960s), civil defense was a cornerstone of national security in the United States. This concept extended across all phases of emergency management, including the preparation for, response to, and recovery from an attack on the homeland. Originally, civil defense centered on minimizing the effects of war on the civilian population and dealing with immediate emergency conditions caused by an attack.[2] To this end, civil defense initiatives sought to prepare civilians for large-scale military threats (such as nuclear weapons).[3] Example initiatives include Bert the Turtle's "Duck and Cover" messages developed by the Federal Civil Defense Administration (Figure 1) as well as media campaigns to promote awareness of fallout shelter locations.[4]

Figure 1. Bert the Turtle awareness campaign

Source: "Atomic Advertising in the 20th and Early 21st Centuries: An Exploration of Cultural Attitudes Towards Nuclear Science and Technology in Advertising and Packaging from 1910 to 2010," National Museum of Nuclear Science & History, https://www.nuclearmuseum.org/virtual/vex1/7231661D-DAEF-44B9-8DB7-532965278021.htm.

As the Cold War ended, the term *civil defense* fell out of use by federal, state, and local governments, and designated civil defense entities merged into modern-day emergency management agencies. Over the next decades, emergency management efforts evolved to focus on evolving hazards and incidents. For example, terrorism prevention became the focus of emergency management efforts following the September 11 attacks.[5] After Hurricanes Katrina and Rita in 2005, efforts shifted toward regional planning for large natural disasters. During the H1N1 pandemic in 2009, the focus shifted toward public health emergency preparedness.[6]

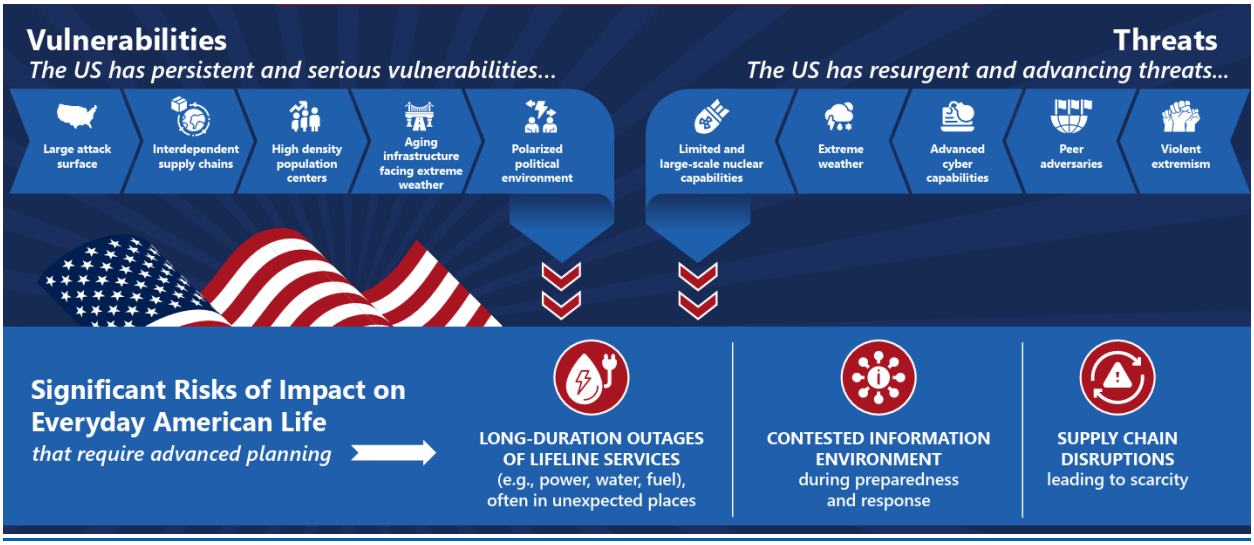
In 2011, Presidential Policy Directive 8 (PPD-8) (a.k.a. Homeland Security Presidential Directive-8) called for an "all-hazards" approach to national preparedness.[7] PPD-8 directed the creation of the National Preparedness Goal, which defines core capabilities and sets priorities for federal preparedness grant programs, training requirements, and exercise programs nationwide.[8] The National Preparedness Goal was built on an all-hazards framework that encompasses natural hazards, terrorism, pandemics, and cyber and industrial incidents; however, it does not include distinct planning scenarios involving a nation-state military attack or coercion, even though the US is currently facing threats that demonstrate the need for one.

Why Should the US Refocus on Civil Defense?

Today, the nation faces an evolving and heightened risk of attacks on its people, supply chains, and critical infrastructure. Nation-state adversaries have demonstrated both the capability and intent to execute cyber-attacks, information operations, and sabotage on US critical infrastructure and citizens, and long-range strategic and small tactical nuclear weapons remain threats.[9] Reflecting the severity of these threats, the Trump Administration's June 2026 National Resilience Strategy declared that preventing any adversary or hazard from holding America's core interests at risk is a central national priority.[10]

Protecting the homeland is harder now than it was a decade ago. Social media and advances in artificial intelligence have created a contested information environment that criminals, insiders, and nation-state actors can exploit. Extreme weather events are hitting harder, more often, and in places whose built environments are not prepared, from mountain communities facing flooding previously experienced only on coasts to northern grids facing extreme heat. Many jurisdictions rely on aging infrastructure built to standards that no longer match the hazards they face (see Figure 2). [11]

Figure 2. Current vulnerabilities, threats, and risks of disruptions to American lives



Source: CNA.

At the same time, defense and response capacity face structural constraints. The National Guard and other disaster-response partners may be unavailable for consequence management at home if they are supporting military operations overseas. Much of the critical infrastructure the country depends on is privately owned, globally distributed, and only partially under government control. That same infrastructure

sustains military installations, ports, data centers, and defense-industrial sites, so disruptions carry direct national security consequences. The companies operating it may not consider themselves at risk of nation-state attack, but adversaries seeking to weaken the United States may specifically target them.

As these threats demonstrate, the US is vulnerable to multiple forms of adversary pressure, including military force, coercive economic statecraft, critical system compromise, and disruptions of the flow of goods and services that communities rely on every day. A renewed civil defense framework must anticipate this full range of threats.

What Should the US Focus On?

In this changing threat landscape, the US would benefit from paying renewed attention to some tenets of the original civil defense initiatives. Today, The CNA Corporation (CNA) proposes a civil defense framework that comprises three critical areas: **providing population support and consequence management**, **protecting economic vitality and critical infrastructure**, and **maintaining public cohesion and will**.

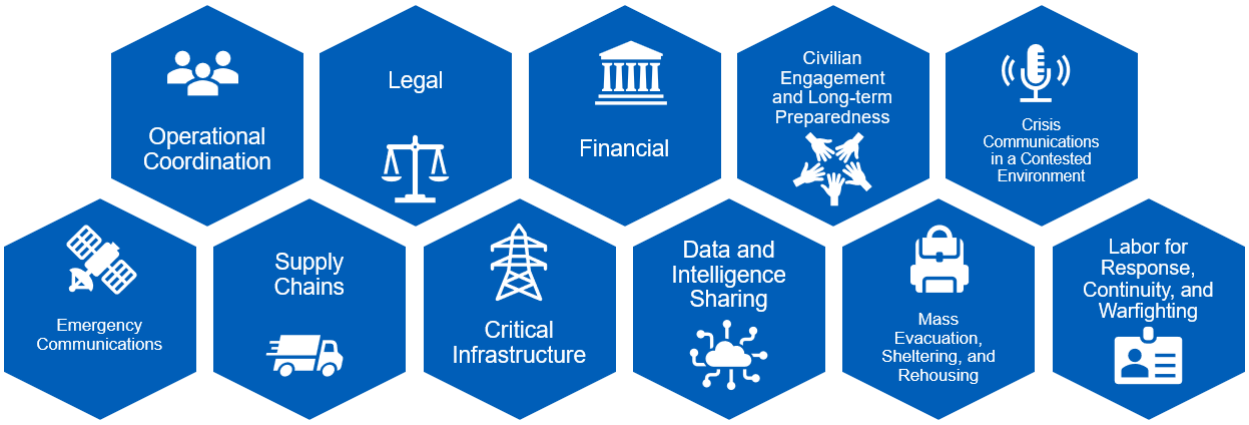
These tasks are not easy, and executing them will require numerous resources, a wide range of skill sets, and anticipation and acceptance of scarcity in personnel, supplies, and functioning infrastructure during and after major incidents. To this end, increased and renewed partnerships and coordination will be required between the public sector, US citizens, and the private sector.

To help drive these efforts, CNA developed this report to address the first critical area: providing population support and consequence management during responses to complex incidents, including long-duration, widespread outages of critical infrastructure. This report identifies gaps in civil defense planning and offers potential solutions across all three critical areas.

Challenges and Potential Solutions

CNA's homeland security, consequence management, and defense analysts collaborated to aggregate current civil defense challenges and their potential solutions. In the following sections, we highlight gaps in civil defense planning in 11 key areas, examine the potential consequences of these gaps, and propose actionable solutions. These discussions are designed to broaden perspectives on the evolving threats that nation-state actors pose to national security and to illustrate how a robust civil defense strategy can enhance the nation's preparedness and resilience.

Figure 3. Civil defense planning focus areas



Source: CNA.

Operational coordination

Current emergency management organizational structures and capacities have proven insufficient for large-scale and protracted emergency responses. During geographically broad and sustained emergency response and recovery, existing structures will be challenged by conflicting jurisdictional authorities, incomplete situational awareness, and a lack of resources to ensure sustainability over extended periods. Furthermore, local emergency management agencies, public health departments, and related organizations often operate with limited personnel and resources. During an emergency response, these organizations will need to undertake the parallel tasks of restoring disrupted lifeline services, managing cascading consequences, and maintaining continuity of government. Most local emergency management organizations are not currently designed or resourced to address all of these demands, so finite resources—including organizational capacity—will be stretched. For example, when Hurricane Helene struck six states in September 2024, each state managed its own emergency operations center activation. Existing unified operational structures above the state level (i.e., the Regional Response Coordination Center, the National Response Coordination Center, and the Emergency Management Assistance Compact) were not designed

to account for the scale and simultaneity of competing demands for mutual aid, personnel, and other shared resources across state lines. State and local agencies simultaneously struggled to sustain 24-hour operations. Local coordination challenges were particularly evident in larger jurisdictions where multiple agencies were operating.

Given that the majority of critical infrastructure in the US is privately operated, emergency responses may also involve the private sector. However, current frameworks for sharing situational awareness and operational coordination are primarily for traditional emergency management partners and do not adequately incorporate the private sector or other nongovernmental partners into the overall response in a coordinated fashion. The government often defaults toward directing rather than collaborating with private-sector actors during emergency situations; however, no command and control authority exists between the government and most private-sector entities. This gap in collaboration may hinder the alignment of actions and the sharing of resources during emergencies. Coordination challenges are particularly concerning if private companies manage critical infrastructure or essential services because delays in response could have cascading effects on public safety and well-being. Coordination is further complicated by real or perceived limitations in how public-sector resources can be used to support the restoration or recovery of private companies' operations, even when those companies provide services or commodities essential to the public good, such as groceries or fuel.

During high-profile incidents (e.g., the COVID-19 pandemic), elected and appointed officials are more likely to assert their role in emergency responses. Incorporating jurisdictional leadership into response efforts can be challenging if coordination structures are not established and if the response extends to governmental entities not traditionally involved in response (e.g., departments of education, departments of commerce). In addition, political leaders are often minimally involved in routine preparedness activities and unfamiliar with emergency response plans. This disconnect can lead to conflicts between emergency management professionals and elected officials, and it can result in courses of action that do not follow established policies and procedures.

Finally, local, state, and national emergency managers rarely exercise their ability to coordinate during large-scale, long-duration incidents, especially those involving critical infrastructure disruptions or utility outages.[12] Overall, the US requires a strategy to adequately coordinate all those who would need to be involved during large-scale and protracted incidents, including the general public, governmental entities (civilian and military), nongovernmental organizations, jurisdictional leadership, and the private sector.

Solutions and recommendations

Recommendation	Actor(s)
Create a national "total defense" plan that integrates a whole-of-society approach informed by international models.[a] *Total defense* refers to a national security approach in which the military, government, the private sector, and citizens share responsibility for defending the country against armed conflict, hybrid threats, and major crises.	Federal
Establish a unified federal structure with dedicated leadership to align national security, infrastructure, and resilience efforts.	Federal
Support state and local civil defense program development; encourage alignment with a national strategy while leveraging leading state models.[b]	Federal, state, local
Update operational coordination plans (including concepts of operations and emergency operations plans) to include increasingly catastrophic planning and scalability as well as structures to rapidly integrate a broader base of government capabilities and partnerships.[c, d]	Federal, state, local
Integrate private-sector, nonprofit, and community-based[e] organizations into meaningful operational coordination, rather than command relationships that do not reflect how most real-world private-sector responses occur.	Federal, state, local, private sector
Enhance command and control frameworks for military and multijurisdictional government response by expanding existing structures (e.g., Dual Status Commanders) and formalizing unified command approaches for scenarios requiring a civil defense response, including military integration as appropriate.	Federal, state
Institutionalize leadership engagement in emergency management by regularly testing responses to long-duration and complex incidents and actively involving political leadership in planning efforts and exercises.[f]	Federal, state, local

Source: CNA.
[a] Alexander Noyes and Jesse Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*, Brookings, 2025, https://www.brookings.edu/articles/why-the-us-needs-a-total-defense-strategy-based-on-resilience/.
[b] Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*, 2018, https://securethegrid.com/community-based-civil-defense-organization/; Virginia Department of Emergency Management, Civil Defense: From the Cold War to Contemporary Threats, 2025, https://dev.vdem.virginia.gov/wp-content/uploads/2024/11/civil-defense-from-the-cold-war-to-contemporary-threats.pdf; Texas Legislature, S.B. No. 2312, Chapter 438. Texas Advisory Committee on Geopolitical Conflict, 2025, https://capitol.texas.gov/tlodocs/89R/billtext/html/SB02312F.htm.
[c] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.
[d] Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[e] Kyle Shideler and Tommy Waller, *Bring Back Civil Defense*, Center for Security Policy, 2022, https://centerforsecuritypolicy.org/wp-content/uploads/2022/03/Civil-Defense-V2.pdf.
[f] Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.

Legal authorities, regulations, and precedent

The legal foundation for civil defense is grounded in the Constitution's preamble, which empowers Congress to "insure domestic tranquility, provide for the common defense, [and] promote the general welfare."[13] This authority has historically been interpreted to include civilian protection through legislation such as the Civil Defense Act of 1950, which granted the federal government broad powers over population movement, public order, and emergency preparedness during the Cold War.[14] However, that act was repealed in 1994,

with its remaining authorities incorporated into Title VI of the 1988 Stafford Act and subsequently assumed by the Federal Emergency Management Agency (FEMA). These responsibilities have largely remained dormant because of a national shift from civil defense toward emergency management focused primarily on natural disasters.[15]

In addition to the Civil Defense Act's successor authorities, the Defense Production Act (DPA) of 1950 contains two authorities relevant to civil defense. Title I authorizes the government to compel the private sector to prioritize the production of critical infrastructure components and emergency supplies, enabling the government to address shortages and maintain essential services during emergencies.[16] Title VII authorizes voluntary agreements between government and industry actors to coordinate production, distribution, and information-sharing decisions in advance of a crisis, with limited antitrust protection for participants.[17] Despite their availability, these authorities have been invoked infrequently because they carry significant political, economic, and coordination implications.[18]

Despite the historical legal precedent, a central challenge for modern scholars, lawmakers, and emergency management professionals seeking to revitalize civil defense in today's evolving threat environment is the absence of a clear and uniform legal definition of *civil defense*.[19] Without a nationally agreed-upon definition and without federally mandated civil defense statutes for state, local, and private-sector entities, civil defense efforts face a high risk of fragmentation. Wide variations in jurisdictional priorities, resource availability, and civil defense subject matter expertise contribute to inconsistent levels of preparedness and engagement across jurisdictions and sectors, ultimately resulting in an insufficiently coordinated national readiness capability.[20]

Modern emergency management, unlike historical civil defense, is largely exercised under police powers, which are held by the states rather than the federal government.[21] This division has become a source of friction because the distinction between a historically federally held defense function and a historically state-held emergency management function has sometimes become blurred during emergency response.

This legal ambiguity also extends to the private sector, where critical infrastructure companies, such as utilities, telecommunications, and supply chain entities, have historically been insufficiently integrated into civil defense, homeland security, and emergency management legal statues.[22] This disconnect is partially the result of two factors. First, laws limit the government's ability to support or intervene in privately owned infrastructure during major disruptions. Second, private-sector operators often compete with one another, which creates disincentives to share threat information, vulnerabilities, and lessons learned across the sector. In addition, modern federal and state laws neither require nor sufficiently incentivize private-sector entities to integrate civil defense principles into their operational and emergency planning. This gap is particularly critical because prolonged disruptions to critical infrastructure would significantly increase the risk of adverse outcomes for the communities these entities serve.[23]

The US has historically placed a strong emphasis on protecting civil liberties. However, effective civil defense relies on the active participation of volunteers, private-sector entities, and civilians,[24] who may be required to enforce preparedness measures, obey unpopular evacuation orders, and abide by emergency movement

restrictions. These potential response actions raise complex constitutional questions, especially in the era of increased public scrutiny due to social media.

Solutions and recommendations

Recommendation	Actor(s)
Conduct a comprehensive inventory and crosswalk of state and federal authorities to identify gaps and opportunities for improved civil defense coordination.	Federal, state
Use DPA Title VII authority to establish pre-crisis information-sharing agreements with industry in priority lifeline sectors, beginning where delegation already aligns with sector-coordination roles.[a, b]	Federal
Amend Title VII of the DPA to deconflict federal coordination with the private sector by working within existing coordination bodies, such as the Cybersecurity and Infrastructure Security Agency's Alliance of National Councils for Homeland Operational Resilience – Critical Infrastructure, to avoid duplicating existing public-private coordination mechanisms.	Federal
When legal clarification is needed, pursue it through FEMA guidance and existing statutory frameworks rather than new legislation.[c]	Federal

Source: CNA.
[a] US Cyberspace Solarium Commission, *March 2020 CSC Report*, Mar. 2020, accessed May 1, 2026, https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/.
[b] Virginia Department of Emergency Management, *Overview and Application of the Defense Production Act*, 2024, accessed May 1, 2026, https://dev.vdem.virginia.gov/wp-content/uploads/2024/10/white-paper-3-overview-and-application-of-the-defense-production-act.pdf.
[c] Rick White, Arthur J. Simental, and John Holst, *21st Century Homeland Defense & Civil Defense*, Homeland Defense Institute, 2023, https://tacda.org/wp-content/uploads/2024/02/21st-Century-Homeland-Defense-and-Civil-Defense-by-Arthur-Simental-Rick-White-and-John-Holst.pdf.

Funding civil defense

Civil defense lacks sustained, dedicated funding streams at any level of government.[25] Federal preparedness grant programs aimed at the state and local levels, including FEMA's Urban Area Security Initiative, direct the large majority of their resources toward law enforcement capabilities and information-sharing infrastructure rather than civil defense activities. This prioritization reflects the origins of the current grant and capacity-building infrastructure: the Homeland Security Grant Program (HSGP). This program was established in the years following September 11, and it still directs a statutorily mandated share of its funding toward law enforcement terrorism-prevention activities; it has not been substantially reoriented toward the wide-area, long-duration infrastructure disruptions described throughout this report. Programs built around catastrophic and regional planning, such as the Regional Catastrophic Preparedness Grant Program (RCPGP), offer a closer starting point but have not yet extended their scopes to wide-area disruptions driven by nation-state actors. Funding for civil defense at the local and state levels is further challenged by budgetary constraints, competing priorities, and lack of political will.[26]

The private sector also faces significant financial disincentives to funding civil defense efforts, including limited eligibility for federal grants.[27] Ambiguity surrounding insurance coverage (especially cyber insurance coverage) complicates information sharing and decision-making during cyber or physical attacks on critical infrastructure.[28]

At the household and community level, financial constraints are an underappreciated barrier to civil defense preparedness. Many individuals have limited financial reserves and rely on continuous access to electronic payment systems for wages, benefits, and daily transactions. When those systems are disrupted during major incidents, people can lose access to the income and funds they need to buy essential goods and services, even if the money is technically in their accounts. And many households do not have the finances to maintain a stockpile of emergency food and other supplies. These constraints significantly reduce preparedness and exacerbate the difficulties individuals and households may experience during a civil defense event.

Solutions and recommendations

Recommendation	Actor(s)
Reorient existing post-9/11 preparedness grant and capacity-building programs, led by the HSGP and extended through the RCPGP and federal training and exercise programs, to prioritize planning considerations and capability requirements for wide-area, long-duration disruptions to lifeline infrastructure.	Federal
Advocate that the National Preparedness Goal be revised to explicitly incorporate nation-state adversarial threats as a distinct planning scenario, considering that the goal's core capabilities and priorities directly shape how HSGP, RCPGP, and other federal capacity-building programs allocate funding.[a]	Federal
Update legislation to address funding and statutory limitations affecting the Department of Homeland Security and FEMA.	Federal
Establish clear emergency funding protocols for civil defense incidents, including those involving privately owned critical infrastructure.	Federal, state, local, private sector
Legislate limits and parameters for cyber insurance coverage of critical infrastructure; more specifically, integrate cyber insurance considerations into incident response frameworks.	Federal
Expand traditional economic recovery plans to incorporate potential economic safeguards, strategies for rapidly mobilizing philanthropic funding in the absence of federal support, and approaches for managing large-scale economic recovery and stimulus efforts.	Federal, state
Reassess and broaden the range of partners involved in these plans, such as economic development organizations.	State, local

Source: CNA.
[a] US Federal Emergency Management Agency, *National Preparedness Goal (2nd ed.)*, Sept. 2015, https://www.fema.gov/sites/default/files/documents/fema_gpd_national-preparedness-goal-2nd-edition_051525.pdf.

Civilian engagement in long-term preparedness

Political divisions and public skepticism toward government initiatives have weakened support for preparedness programs, and outreach from government agencies has been insufficient to encourage broader participation in civil defense–related activities.[29] At the same time, public engagement in preparedness and response efforts has been constrained by low awareness of threats and hazards and limited individual preparedness. The public is largely absent from governmental and military conversations

about US nation-state adversaries (e.g., North Korea, Russia, Iran, China), including their projected capabilities and the situations under which they may act against US national interests.

Many individuals lack the emergency plans and supplies necessary to remain self-sufficient for the recommended 72 hours before government-provided lifeline services are available.[30] And 72 hours of self-sufficiency is likely inadequate to manage long-duration emergencies; a 14-day or longer duration may be required.[31] This gap reflects more than an outdated number. Nations with sustained civil defense traditions, including Sweden, Switzerland, Finland, Singapore, and Taiwan, treat household preparedness as one element of an integrated framework of emergency preparedness that also includes military planning and infrastructure investment. They frame household preparedness as part of national defense and communicate about it continuously across multiple government channels. US federal outreach through Ready.gov and National Preparedness Month is sustained and substantial, but it treats preparedness as personal disaster readiness rather than as civic contribution to national resilience against adversary threats. Sweden distributes a household preparedness brochure to every home in the country; Finland's civil-defense shelter network, built into the country's bedrock, covers more than 80 percent of the population; and Taiwan has issued three updated civil-defense handbooks since 2022 to its nearly 10 million registered households. To address this gap, US households need to be better prepared to face the broader threat picture.[32]

A lack of essential skills among the general population further compounds the challenges in civilian preparedness. Hard skills critical to emergency response, such as basic first aid, navigation without GPS, and other practical survival skills, are not widely taught or practiced. Community-based programs, such as Neighborhood Watch groups and Community Emergency Response Teams, are helpful for small-scale incidents, but they would have limited effectiveness in addressing the unique demands of catastrophic events and large-scale disruptions.[33] Limited preparedness, unclear communication from authorities, and resource constraints could lead to unrest, hoarding of supplies, and challenges to government authority. Under such conditions, response efforts may be strained not only by the initial incident but also by the need to manage secondary impacts driven by public behavior.

Solutions and recommendations

Recommendation	Actor(s)
Strengthen public readiness and awareness through sustained campaigns, standardized guidance, and promotion of individual emergency planning and long-term self-sufficiency.[a]	Federal, state, local
Study best practices from democratic countries with long histories of including their civilian populations in civil defense; examples include Sweden, Switzerland, Singapore, Finland, and Taiwan, where household preparedness functions as one component of an integrated total defense framework.	Federal
Expand civilian education, training, and service programs by incorporating preparedness into school curricula, delivering crisis response training, and leveraging volunteer organizations and national service models.[b]	Federal, state, local
Promote community-based engagement and bottom-up preparedness by encouraging neighborhood initiatives and exercising approaches that build civic readiness. [c]	State, local
Prepare the public for crisis response by communicating potential government actions, encouraging and organizing active participation, and establishing measures to assess preparedness efforts.[d]	Federal, state, local
Prepare civilians to self-sustain with a personal cache of emergency supplies for 14 days to blunt the negative effects of supply chain disruptions.	Federal, state, local

Source: CNA.
[a] Shideler and Waller, *Bring Back Civil Defense*; Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*; Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[b] Shideler and Waller, *Bring Back Civil Defense*; Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*; Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[c] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*; Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[d] Stephanie Stapleton and Dawn Thomas, *Modern Civil Defense Concept Note*, CNA, 2024; Texas Legislature, S.B. No. 2312, *Chapter 438. Texas Advisory Committee on Geopolitical Conflict*.

Crisis communications in a contested information environment

For the government, communicating clearly and credibly with the public during a large-scale emergency is a foundational requirement of civil defense.[34] However, current public communications systems contain significant gaps that can undermine an effective response when it matters most. For example, existing strategies are insufficient to address rampant false and misleading information.[35, 36] In addition, panic and rumor control capabilities remain underdeveloped, leaving communities susceptible to fear, confusion, and behavioral responses that could complicate response operations.[37] Research on risk communication suggests that high-threat messaging, particularly when not paired with clear guidance on protective actions, can cause audiences to disengage or become emotionally numb rather than respond. Current emergency response and civil defense communications frameworks do not adequately address this tension.[38]

These challenges are being compounded by the erosion of public trust in government.[39] Emergency response and civil defense activities will be greatly degraded if the public does not accept official sources as credible and authoritative.[40] Communications around difficult but necessary measures, such as rationing, curfews, or public health restrictions, are particularly vulnerable to resistance and noncompliance, and

current strategies do not adequately account for how to present unpopular directives in ways that encourage public cooperation.[41] At the same time, public education around receiving and interpreting emergency alerts is weak, leaving many people without foundational knowledge on how to access official guidance and effectively respond. The chaotic information environment further complicates this picture; people are increasingly receiving information through varying channels because of their age, political affiliation, and algorithmic filtering, making broad and consistent messaging difficult to achieve through normal mechanisms.[42]

Questions of authority, coordination, and telecommunications infrastructure survivability add another layer of complexity. In a scenario requiring a civil defense response, it is not immediately clear who at the federal level will control public messaging, how information security considerations will be balanced against the need for public awareness, or what alternative mechanisms would exist if telecommunications infrastructures were degraded or compromised. Existing structures, such as the National Incident Management System (NIMS) Joint Information System and Joint Information Center protocols, provide clear authority and guidance for these decisions during routine tactical incident response, but they offer no comparable criteria for weighing intelligence and national security equities (including protection of sources, methods, or an active attribution investigation) against the public's need to know. In addition, nontraditional trusted voices, including community organizations, faith institutions, employers, and universities, are underutilized as communications partners, despite their potential to reach populations that may be skeptical of government sources.

Solutions and recommendations

Recommendation	Actor(s)
Expand current public information protocols, including NIMS Joint Information System and Joint Information Center authorities, to give designated officials clear criteria for weighing national security equities against public disclosure in scenarios involving nation-state-attributed threats.[a]	Federal
Designate clear federal authority for public messaging during a civil defense response and establish a coordination framework, not a command relationship, for how federal, state, and local officials should align their messaging.[b]	Federal
Identify alternative communications channels and protocols to maintain public messaging capability if telecommunications infrastructure is degraded or compromised.[c]	Federal, state, local, private sector
Counter false and misleading information proactively using research-based strategies, including inoculation and media literacy, that can help individuals identify trustworthy sources and distinguish them from rumors and manipulated content.[d, e]	Federal, state, local private sector
Develop communication strategies for difficult and unpopular measures by preparing guidance for public information officers on how to frame directives such as rationing, curfews, and public health restrictions in ways that acknowledge public concerns, reduce resistance, and maintain cooperation.	Federal, state, local
Before incidents occur, build public trust through innovative, consistent, and transparent engagement between trusted voices and the communities they serve.	State, local
Identify and partner with trusted voices—especially those with established relationships in vulnerable or historically underserved populations, such as community leaders, faith organizations, local fire and law enforcement, and professional associations.	State, local
Develop and codify methods for working with nontraditional partners that can amplify reach, including popular content creators, media organizations, and employer and university networks.	Federal, state, local
Study approaches to reduce panic in a high-information media environment by examining how the framing, timing, platform, and tone of official communications affect public behavior; develop guidance for emergency managers on calibrating transparency against the risk of behavioral overreaction.[f]	Federal

Source: CNA.

[a] CNA, "Civil Defense: From the Cold War to Contemporary Threats," 2025, https://www.cna.org/quick-looks/2025/08/Civil-Defense-From-the-Cold-War-to-Contemporary-Threats.pdf.

[b] Dawn Thomas, Braeanna Hillman, Olga Thomas, and Christine Huges, *Civil Defense Considerations for OPNAV at War*, CNA, 2025.

[c] CNA, "Civil Defense: From the Cold War to Contemporary Threats."

[d] Megan K. McBride, Pamela G. Faber, Kaia Haney, Patricia J. Kannapel, and Samuel Plapinger, *Best Practices for Countering Malign Influence*, CNA, DIM-2025-U-041133-Final, 2025, https://www.cna.org/reports/2025/04/Best-Practices-for-Countering-Malign-Influence.pdf.

[e] CNA, "Civil Defense: From the Cold War to Contemporary Threats."

[f] Stapleton and Thomas, *Modern Civil Defense Concept Note*.

Emergency communications

In the US, emergency communications depend heavily on privately owned telecommunications infrastructure. If this infrastructure fails or is deliberately disrupted, authorities may be unable to issue emergency alerts, news outlets may be unable to disseminate timely information, and responders and government agencies may lose the ability to coordinate logistics, distribute resources, and maintain command and control. The loss of these capabilities would severely degrade incident response and leave

communities without reliable access to lifesaving information. These systems and the infrastructure that supports them (e.g., internet, cell phone networks) could be disrupted or deliberately targeted during major incidents with major consequences for individuals, communities, and the government.[43] The same telecommunications systems also underpin critical infrastructure operations, financial transactions, and many other aspects of daily life. Additional risk is introduced by dependencies on space-based infrastructure. In particular, GPS satellite systems and subsea cables provide essential navigation, communications, and information-sharing capabilities; however, these dependencies are not fully understood and lack robust backup.[44] Disruptions to these services could have cascading effects across multiple sectors.[45] When available, backup communication systems often lack key capabilities, such as geo-targeting and multilingual and accessible features, reducing their reach across diverse populations.

Current approaches to planning for large-scale communication outages focus on maintaining communication among first responders; they address the need to communicate with the public in only a limited way.[46] Some backup telecommunications systems include FirstNet, satellite phones, the Government Emergency Telecommunications Service, the Wireless Priority Service, and the Integrated Public Alert and Warning System (connected to National Oceanic and Atmospheric Administration (NOAA) weather radios). However, other than the NOAA radio (which few households own), the use of these systems is limited to first responders. In addition, public alerting systems are often outdated, inconsistently implemented, and not integrated with federal platforms, such as the Integrated Public Alert and Warning System (IPAWS). The limited emergency communications capabilities and capacities at all government levels (local, state, and federal) are inadequate to meet the needs of a large-scale telecommunications outage.

The lack of independent emergency communications mechanisms and backup communications capabilities has led to heavy reliance on privately owned telecommunications infrastructure. Coordination between the government and private-sector partners is inconsistent, limiting unified planning and prioritization during crises. This reliance raises additional concerns regarding access, resilience, and decision-making in high-demand or contested environments.

Solutions and recommendations

Recommendation	Actor(s)
Strengthen the resilience of emergency communications by identifying secondary and tertiary mechanisms for information sharing.	Federal, state, local, private sector
Develop plans that account for the possibility that local accounts, emergency systems, or public-facing channels may be spoofed or hacked.	Federal, state, local
Develop resilient communication strategies for degraded environments by establishing plans, standards, and backup methods to ensure continuity of public messaging.[a]	Federal, state, local
Build redundant and alternative communication capabilities by investing in diverse technologies, stockpiling equipment, and promoting community-based systems, such as amateur radio.	Federal, state, local private sector
Modernize and integrate mass alerting systems by enhancing IPAWS capabilities and improving accessibility.	Federal
Assess and enhance infrastructure resilience by evaluating vulnerabilities in space-based and critical communications systems, developing backups, and implementing hardening strategies.[b]	Federal, private sector
Strengthen coordination with private and nontraditional partners by integrating stakeholders into planning and establishing agreements for deployable communication assets during outages.[c]	Federal, state, local private sector
Expand research, training, and federal coordination to improve the use of alternative communication tools and protect critical systems through collaboration between the Department of War (DoW), civilian agencies, and the private sector.[d]	Federal, private sector

Source: CNA.
[a] Dawn Thomas, *Planning for Continuity in the Face of a Cyber-Attack: Challenges and Best Practices*, CNA, 2021; Dawn Thomas and David Knoll, 21st Century Consequence Management Planning: What's Different, What's the Same, and Why We Need to Step Up Our Game, CNA, 2025.
[b] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[c] Thomas, *Planning for Continuity in the Face of a Cyber-Attack: Challenges and Best Practices.*
[d] Stapleton and Thomas, *Modern Civil Defense Concept Note*; Thomas, Hillman, Thomas, and Huges, *Civil Defense Considerations for OPNAV at War.*

Supply chains

Individuals, governments, and private-sector entities—including those in critical lifeline sectors such as grocery and health care—depend on supply chains and just-in-time processes that are efficient by design but fragile under stress. When these systems are disrupted or deliberately targeted, the production, procurement, and distribution of essential goods can break down quickly during emergencies. The interconnected nature of producers and consumers creates complex supply chains with hidden vulnerabilities. Modern supply chains rely heavily on telecommunications, information technology (IT), operational technology, digital financial systems, and continuous capital flows; disruptions in any of these areas or in source materials can worsen shortages during crises. For this reason, supply chains are prime targets for adversaries.

Stockpiles of essential goods are often limited at points of sale; as a result, individuals and organizations would have difficulty sustaining operations amid the prolonged disruptions of a large-scale emergency. If large emergency stockpiles are lacking, production must be agile enough to quickly shift to critical goods.

However, the private sector faces challenges in rapidly adapting production lines, with limited knowledge about which materials will be needed, who can pivot production, and how such shifts would be funded or incentivized. This uncertainty complicates planning. Supply chain data are privately held, which can also hinder situational awareness and coordinated response.

Certain supply chains, especially within the defense industrial base, are particularly vulnerable because of reliance on complex and often external suppliers. Although efforts are underway to identify critical components and suppliers, these efforts remain immature, leaving gaps in protecting essential capabilities. For example, many medical supplies and computer chips may be in higher demand during wartime, but they may be difficult to supply because they are often imported.[47]

Crises also disrupt supply and demand dynamics, as was seen during the COVID-19 pandemic. Demand for typically low-demand commodities can suddenly spike, overwhelming production capacity. Multiple sectors and governments might compete for limited resources, causing price volatility. Without national frameworks to prioritize resource allocation, distribution during large-scale incidents remains uncertain.

Finally, current logistics and distribution systems limit effective emergency response. Local logistics and resource management are not built for sustained large-scale crises, restricting resource movement. Although private-sector logistics could help, integration with emergency management is limited. National transport and delivery systems may also be overwhelmed or disrupted, and these challenges would be worsened by damaged infrastructure.

Solutions and recommendations

Recommendation	Actor(s)
Map critical supply chains to identify vulnerabilities (e.g., single-source vendors, foreign dependencies) and evaluate risks across supplies, equipment, digital systems, and personnel.[a]	Federal, private sector
Focus on supplies critical to DoW operations and civilian lifeline services, including their supply chain dependencies, domestic production capacity, stockpiles, and distribution networks.[b]	Federal
Build supply chain working groups and partnerships between neighboring jurisdictions to improve regional coordination, situational awareness, and the sharing of resources and information.	State, local
Diversify and expand sourcing options by identifying alternative and just-in-time suppliers, establishing prenegotiated agreements such as priority-of-supply contracts, standing procurement contracts, and mutual aid arrangements with private suppliers, and leveraging nontraditional and local partners to meet critical needs.[c]	Federal, state, local, private sector
Leverage public-private coordination and authorities by strengthening partnerships with the private sector, identifying opportunities to shift supply channels (e.g., retail to commercial), and assessing local and state application of the DPA.[d]	Federal, state, private sector
Enhance logistics and distribution capabilities by investing in emergency management logistics, increasing surge capacity for procurement and delivery, and developing plans to operate in degraded communications and transportation environments.	Federal, state, local
Assess and optimize stockpiling and production strategies by evaluating existing federal, state, local, tribal, and territorial supply caches; considering localized production and storage; and conducting cost-benefit analyses of centralized warehousing and distribution models.	Federal, state, local
Improve resource prioritization mechanisms by establishing processes to validate externally sourced goods and identifying critical components (e.g., semiconductors, transformers) for targeted supply stabilization and allocation.	Federal
Decrease supply-chain pressures by developing public campaigns to reduce demand for critical goods and services during times of national crisis.	Federal, state, local, private sector

Source: CNA.
[a] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.; Texas Legislature, S.B. No. 2312, *Chapter 438. Texas Advisory Committee on Geopolitical Conflict*.
[b] Texas Legislature, S.B. No. 2312, *Chapter 438. Texas Advisory Committee on Geopolitical Conflict*.
[c] Texas Legislature, S.B. No. 2312, *Chapter 438. Texas Advisory Committee on Geopolitical Conflict*; CNA, "Civil Defense: From the Cold War to Contemporary Threats."
[d] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*; Thomas and Knoll, *21st Century Consequence Management Planning*.

Critical infrastructure

The essential services that Americans rely on—from electricity and water to communications and transportation—depend on an interconnected system of critical infrastructure that serves both civilian populations and national defense operations. Disruptions to critical infrastructure assets can severely degrade force projection, the defense industrial base, and civilian services, making these assets desirable targets. For example, attacks on key transportation nodes (e.g., ports, airports, rail hubs, trucking facilities) can create bottlenecks that constrain the movement of resources needed for both civilian populations and military operations.

Many critical infrastructure assets are privately owned and operated, reducing direct government control during emergencies and creating potential misalignment between public- and private-sector priorities. In addition, critical infrastructure owners and operators have not been consistently integrated into federal, state, and local planning and response structures, exacerbating coordination challenges. This lack of integration is particularly apparent during high-consequence events, especially if owners, operators, and the public sector face emerging threats, such as cyberattacks or uncrewed aerial systems (UASs).[48, 49]

Many public- and private-sector entities have not planned for major disruptions to vulnerable critical infrastructure systems. Current plans focus on restoration but fail to account for large-scale rebuilding due to extensive damage (as was required for the power grid in Puerto Rico after Hurricane Maria).[50] Continuity planning for these prolonged disruptions is similarly limited, especially for widespread power and water outages.[51] These gaps, combined with shortages of trained personnel and infrastructure equipment, leave the United States ill-prepared to withstand long-term critical infrastructure outages during large-scale incidents.[52]

Solutions and recommendations

Recommendation	Actor(s)
Strengthen public-private coordination and planning by solidifying partnerships, aligning critical infrastructure priorities, and creating frameworks for mission assurance to integrate DoW and non-DoW dependencies.[a]	Federal, state, local, private sector
Map critical infrastructure systems and dependencies at the national, state, and local levels to identify potential points of failure and to prioritize critical services (e.g., food, fuel, energy, medical supplies) to improve visibility and risk analysis.	Federal, state, local, private sector
Invest in, prioritize, and harden infrastructure and cybersecurity through modernizing, building disaster-resilient systems, and enhancing cybersecurity for publicly owned utilities.[b]	Federal, state, local, private sector
Incentivize resilience through policy and contracts by implementing such mechanisms as cost-sharing agreements for operators that maintain continuity plans, validate capabilities, and participate in exercises.[c]	Federal, state, private sector
Enhance continuity and catastrophic recovery planning by developing and exercising long-duration outage strategies, data loss plans, and system reconstructions.[d]	Federal, state, local, private sector
Improve restoration capacity and partnerships by pre-identifying private sector partners to support infrastructure repair and recovery following cyber or physical disruptions.[e]	Federal, state, local, private sector
Address emerging threats and vulnerabilities by investing in counter-UAS capabilities, potentially centralizing this capability at the national level to gain efficiencies for state and local jurisdictions.[f]	Federal, state, local, private sector

Source: CNA.

[a] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*; White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense*.

[b] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*.

[c] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*.

[d] Shideler and Waller, *Bring Back Civil Defense*; Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.

[e] CNA, "Civil Defense: From the Cold War to Contemporary Threats."

[f] Jeffrey Kucik, Jerry Meyerle, John Milton, and Yee San Su, *CNA Maritime Dialogue: US Commercial Ports During a Wartime Mobilization*, CNA, CCP-2025-U-043199-Final, 2025.

Data and intelligence sharing

Outdated systems, fragmented coordination, and insufficient integration of key stakeholders undermine the nation's ability to prevent major kinetic or cyberattacks. Current intelligence-sharing structures between local law enforcement and federal or military intelligence agencies were largely designed during the global war on terror and are therefore structured with a bottom-up rather than top-down approach. They are too slow and lack the granularity to meet the demands of real-time information needs, limiting their ability to deliver actionable intelligence to field-based law enforcement during rapidly evolving incidents. Accurate analysis, such as that from intelligence analysts and meteorologists, is essential to identify emerging disasters and threat landscapes, but information sharing may be fragmented or delayed if federal agencies supporting these activities are constrained in their personnel and funding.[53] Compounding this issue, intelligence collection and analysis are not always focused on the most critical sectors or targets for localities, such as vulnerable populations.

Significant gaps in intelligence sharing also exist between jurisdictions. Threats, disruptions, and disasters frequently cross jurisdictional borders, but political divisions, incompatible technologies, and fragmented systems often complicate cooperation and information exchange. These barriers are particularly problematic during emergencies, when rapid coordination is essential. As threats grow more complex and incidents unfold at greater speeds, local authorities may find themselves unable to access timely and relevant intelligence through existing channels, leaving them unprepared to respond effectively.

Finally, as the number of potential targets expands, new or ad hoc partners in the response effort may lack access to secure communication tools or clear guidance on which platforms to use, further complicating coordination. Private-sector partners are often inconsistently integrated into intelligence-sharing processes despite possessing relevant data, operational insights, and infrastructure capabilities. This lack of integration creates uncertainty about how private-sector entities should engage during emergencies, particularly with respect to early warning systems and threat alerts. Without a clearly defined mechanism linking businesses to threat alerts and intelligence flows, private-sector actors may remain unaware of emerging threats or unsure of how to respond effectively. Barriers such as limited security clearances for private-sector personnel and restrictions on sharing and leveraging private-sector data further hinder the ability to share and use this critical information.

Solutions and recommendations

Recommendation	Actor(s)
Increase the adoption of secure, interoperable platforms for intelligence sharing (e.g., the Homeland Security Information Network).	Federal, state, local
Create intelligence-sharing processes that move quickly during conflict or protracted war (e.g., top-down, centralized, decentralized).	Federal, state, local
Integrate data and intelligence analysts into emergency operations center staffing and provide leadership and oversight of these activities prior to and during an emergency (e.g., through a chief data officer).	State, local
Ready data and data systems by identifying essential data needs for civil defense emergency response at all levels of government. Ensure systems can identify and integrate future data.	Federal, state, local
Engage IT personnel and services as key players in emergency response plans and emergency operations center activations. Chief technology officers and other technology leaders can help guide strategic and tactical technology acquisitions prior to and during emergencies and should also be incorporated into planning efforts.	Federal, state, local

Source: CNA.

Mass evacuation, sheltering, and rehousing

Extreme weather and attacks from more capable adversaries could lead to incidents requiring mass evacuation and mass sheltering. Emergency and consequence managers will face several challenges implementing these operations on a large scale. At the national level, the US lacks frameworks and strategies to guide decisions and operations for mass evacuations and displacements, such as how to balance shelter-in-place orders with evacuations and how to manage and house many displaced individuals. Furthermore, there is no integrated system for tracking displaced populations or facilitating family reunification.

For evacuations, federal entities lack the authority to mandate evacuations, leaving the decisions to state and local governments. However, evacuation laws, thresholds, and enforcement mechanisms vary widely across jurisdictions,[54] creating implementation and coordination challenges. Even where evacuation authorities are clearly established, effective large-scale evacuations may be difficult or impossible to enforce because they rely heavily on voluntary compliance, which is influenced by public perception, risk awareness, and access to transportation. Preparedness levels also vary significantly across the nation, with jurisdictions that have limited experience managing hazards such as wildfires or hurricanes often struggling to develop and execute effective evacuation plans.

For shelters, jurisdictions have capacity limitations (for personnel, facilities, and materials) that can prevent the development of adequate plans to shelter their populations after a large-scale disaster, especially one affecting multiple local jurisdictions, states, or regions.[55] Evacuation and shelter plans are also not usually coordinated across jurisdictions, and this lack of strategic alignment can create inconsistencies in planning assumptions and response actions. Further, the public tends to resist both evacuation and official sheltering directives, although they do so for different reasons. Mandatory evacuation orders have a compliance rate of between 30 and 70 percent across hazards. Evacuation can be costly and can be logistically challenging for those in poor health, the elderly, the disabled, those with children, and those with pets. Risk perception

and communication also play a strong role. Congregate sheltering is often viewed negatively, with concerns over safety, privacy, and whether shelters can adequately meet the needs of the individual. As a result, many individuals may seek alternative or informal sheltering arrangements, complicating emergency managers' ability to maintain situational awareness and deliver essential services.[56, 57]

Solutions and recommendations

Recommendation	Actor(s)
Develop a comprehensive national strategy for mass displacement that integrates evacuation and sheltering solutions, including considerations for large-scale population movements and refugee integration.[a]	Federal
Strengthen evacuation planning and operational capabilities across all levels of government by supporting coordinated planning efforts and identifying mechanisms for state and federal support to large-scale evacuations, including clarifying the role of FEMA.[b]	Federal, state, local
Establish integrated housing strategies at the state and local levels to address emergency sheltering needs for large populations. These strategies should leverage private-sector housing and partnerships, explore innovative approaches (e.g., crowdsourced housing, sheltering solutions), and reevaluate mass congregate sheltering models with post-COVID-19 considerations.	State, local, private sector
Enhance coordination between emergency management and housing agencies within and across states to better align response and recovery efforts and accelerate transitions to stable housing.	State, local

Source: CNA.
[a] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense*.
[b] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense*; Stapleton and Thomas, *Modern Civil Defense Concept Note*.

Labor for response, continuity, and warfighting

Current emergency response planning approaches assume that the government will lead the response, beginning at the local level and elevating to higher levels of government as incidents overwhelm the capacities of lower levels of government. In addition, localities and states assume the federal government will play a large role in widespread, long-duration emergencies. However, recent events—including the COVID-19 pandemic and the 2025 and 2026 federal government shutdowns—have demonstrated the limits of federal government support. If the federal government's resources and personnel are occupied with a war abroad, states and localities might be required to respond and recover with minimal federal support.

Ensuring adequate labor to simultaneously support critical societal functions, emergency response, and military operations presents a significant civil defense challenge. Even in peacetime, public safety sectors such as law enforcement and emergency management face persistent staffing shortages; for example, law enforcement agencies operate with an average 10 percent deficit (and a significantly higher deficit in many large cities), and emergency management roles suffer from underfunding and high attrition.[58, 59] These shortages, compounded by burnout from recent pandemic responses and increasing disaster frequency

and severity, risk undermining responders' ability to provide essential services and meet the needs of the incident.

Compounding these challenges is the evolving nature of volunteerism. Spontaneous volunteerism has increased, meaning that people want to "help out when they have time and when the task fits their agenda."[60] At the same time, pre-incident volunteerism has declined. In general, local communities and states lack plans for accepting, organizing, and effectively utilizing large numbers of spontaneous volunteers during emergencies. Volunteer registry systems and credentialing systems are generally fragmented within jurisdictions because they are time-consuming to build and maintain. Existing volunteer systems are also not set up to identify unique skill sets that may be relevant for disaster response beyond general and medical volunteers. Other skill sets, such as cybersecurity, port operations, procurement and contracting, and logistics, are vital to civil defense, but a catalog of such desired skill sets does not exist, nor do jurisdictions solicit for volunteers with those skills.

The complexity of modern warfare further intensifies labor demands. Specialized professionals, such as damage inspectors, IT experts, forensic analysts, and emergency communications operators, will be necessary to address threats from irregular warfare tactics—including malicious use of UAS and emerging space-based technologies, cyberattacks, and chemical, biological, radiological, nuclear, and explosive attacks. The existing workforce is unlikely to meet these specialized needs, and emergency managers must integrate these new mission sets with personnel who have limited prior experience, increasing operational strain.

This strain will be exacerbated when military forces are deployed overseas. The National Guard, often a critical asset for state-level emergency response, may be activated under federal authority (Title 10), rendering them unavailable for state missions (Title 32). This dual demand will reduce domestic capacity to respond to natural disasters or attacks. Moreover, state leadership often lacks visibility into National Guard deployment schedules and civilian job roles, complicating continuity planning. As DoW expands warfighting efforts and production of critical supplies, competition for labor will intensify, further stressing the workforce needed for response, continuity, and defense.

Solutions and recommendations

Recommendation	Actor(s)
Plan for large-scale labor needs by prioritizing key missions, determining essential skills, and designing targeted volunteer training to minimize time and resource burdens.	Federal, state, local
Study underutilized labor pools, such as adults outside the paid workforce (e.g., stay-at-home parents, early retirees), eligible incarcerated populations, seniors, and students, to support civil defense efforts.	Federal, state
Identify incentives to increase public participation in preparedness and response activities.	Federal, state, local
Develop a comprehensive framework to mobilize, train, and deploy spontaneous volunteers effectively; integrate formal volunteer groups while preparing for grassroots participation.	Federal, state, local
Consider the range of support types, including ones that require less time-intensive training or less physical strength.	Federal, state, local
Develop volunteer management systems that can match volunteers with opportunities in real time, letting volunteers select opportunities (i.e., crowdsourcing volunteers based on tasks).	Federal, state, local
Expand emergency management capacity by identifying potential full-time, volunteer, and reserve personnel across all government levels and creating training programs for critical response skills.	Federal, state, local
Explore modern draft options that minimize disruptions to lifeline service workers.	Federal
Establish a national framework for irregular warfare response by identifying required capabilities and coordinating federal, state, local, and private-sector resources.	Federal, state, local, private sector
Promote a national strategy to strengthen state defense forces, aligning their missions, skills, and training to support irregular warfare responses and other critical tasks.	Federal, state

Source: CNA.

Conclusion

Nation-state adversaries, extreme weather events, brittle supply chains, and aging infrastructure are creating the conditions for cascading, long-duration incidents for communities across the country. Addressing these challenges will require sustained effort, new partnerships, and a willingness to plan for scenarios that extend beyond traditional emergency management.

A renewed civil defense approach offers a way forward. By focusing on population support and consequence management, protecting economic vitality and critical infrastructure, and maintaining public cohesion and will, the nation can improve its ability to withstand and recover from major incidents. The 11 areas examined in this report, from operational coordination and legal authorities to supply chains and labor mobilization, represent the scope of work required.

This work also arrives at a moment of opportunity. The administration's National Resilience Strategy, released in June 2026, centers homeland resilience explicitly on the premise that no adversary or hazard should be able to hold America or its core interests at risk.[61] A renewed civil defense approach, as outlined in this report, offers one path toward operationalizing that premise by translating it into concrete capabilities, funding structures, and legal authorities at the federal, state, and local levels.

By offering practical steps that critical infrastructure owners and operators, individual citizens, and federal, state, and local governments can take now to strengthen civil defense, this report provides a starting point. Implemented together, the following measures can help the nation better anticipate future crises, reduce their consequences, and preserve the security and well-being of the American people. The table that follows highlights recommendations and solutions at the federal, state, local, private-sector, and individual levels.

Priority solutions and recommendations

Actor(s)	Recommendation
Federal	Create a nationwide, whole-of-society civil defense strategy that operationalizes the 2026 National Resilience Strategy's adversary-centered resilience priorities. Revise the National Preparedness Goal to incorporate nation-state adversarial threats as a distinct planning scenario. Develop a national strategy for mass displacement. Provide funding for civil defense initiatives, including critical infrastructure improvements. Incentivize individual preparedness. Define governmental authority to intervene in privately owned critical infrastructure (based on DPA). Partner with the private sector to assess supply chain vulnerabilities for critical response resources and essential commodities. Invest in counter-UAS strategies and technologies to support critical infrastructure.
State	Develop civil defense programs aligned to the national strategy. Define state authorities for civil defense. Identify funding for civil defense (pre-incident and response/recovery), including philanthropic funding. Incorporate threats from adversary nation-states into risk assessments. Incentivize individual preparedness. Develop emergency communications plans for degraded communication environments. Develop and promote community-level civil defense programs.
Local	Explore the roles individuals can play in disaster response in the jurisdiction. Establish relationships with critical infrastructure within the jurisdiction. Establish relationships with trusted community messengers and nontraditional response partners. Develop public education campaigns and initiatives for civilian preparedness. Develop emergency communications plans for degraded communications environments. Develop regional supply chain working groups. Expand volunteer management plans and systems to prepare for spontaneous volunteers.
Private sector	Incentivize workforce emergency preparedness. Develop restoration and rebuilding contingency plans for long-duration outages. Identify supply chain vulnerabilities and critical dependencies.
Individual	Prioritize individual preparedness, aiming for 14 days of self-sufficiency. Identify authoritative government sources of information and subscribe to emergency alerts. Develop a household emergency response plan that includes how to communicate in a degraded communications environment. Consider how your skills could support disaster response and recovery and seek out volunteer opportunities.

Source: CNA.

Abbreviations

DoW	Department of War
DPA	Defense Production Act
FEMA	Federal Emergency Management Agency
HSGP	Homeland Security Grant Program
IPAWS	Integrated Public Alert and Warning System
IT	information technology
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
PPD-8	Presidential Policy Directive 8
RCPGP	Regional Catastrophic Preparedness Grant Program
UAS	uncrewed aerial system

Endnotes

[1] "Civil Defense Definition & Meaning," Merriam-Webster, https://www.merriam-webster.com/dictionary/civil%20defense.
[2] CNA, "Civil Defense: From the Cold War to Contemporary Threats," 2025, https://www.cna.org/quick-looks/2025/08/Civil-Defense-From-the-Cold-War-to-Contemporary-Threats.pdf.
[3] CNA, "Civil Defense: From the Cold War to Contemporary Threats."
[4] "Atomic Advertising in the 20th and Early 21st Centuries: An Exploration of Cultural Attitudes Towards Nuclear Science and Technology in Advertising and Packaging from 1910 to 2010," National Museum of Nuclear Science & History, https://www.nuclearmuseum.org/virtual/vex1/7231661D-DAEF-44B9-8DB7-532965278021.htm.
[5] CNA, "Civil Defense: From the Cold War to Contemporary Threats."
[6] CNA, "Civil Defense: From the Cold War to Contemporary Threats."
[7] US Department of Homeland Security, "Presidential Policy Directive / PPD-8: National Preparedness," Mar. 30, 2011, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.
[8] US Federal Emergency Management Agency, *National Preparedness Goal (2nd ed.)*, Sept. 2015, https://www.fema.gov/sites/default/files/documents/fema_gpd_national-preparedness-goal-2nd-edition_051525.pdf.
[9] CNA, "Civil Defense: From the Cold War to Contemporary Threats"; CNA, "Facing 21st-Century Threats: What Every Consequence Manager Should Know," 2025, https://www.cna.org/quick-looks/2025/08/Facing-21st-Century-Threats.pdf.
[10] The White House, *National Resilience Strategy*, June 2026, https://www.whitehouse.gov/wp-content/uploads/2026/06/2026-National-Resilience-Strategy-1.pdf.
[11] CNA, "Facing 21st-Century Threats: What Every Consequence Manager Should Know."
[12] Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*, 2018, https://securethegrid.com/community-based-civil-defense-organization/.
[13] The Preamble to the US Constitution, n.d., https://constitution.congress.gov/constitution/preamble/.
[14] "Statement by the President Upon Signing the Federal Civil Defense Act of 1950," 1951, https://www.trumanlibrary.gov/library/public-papers/10/statement-president-upon-signing-federal-civil-defense-act-1950.
[15] Rick White, Arthur J. Simental, and John Holst, *21st Century Homeland Defense & Civil Defense*, Homeland Defense Institute, 2023, https://tacda.org/wp-content/uploads/2024/02/21st-Century-Homeland-Defense-and-Civil-Defense-by-Arthur-Simental-Rick-White-and-John-Holst.pdf.
[16] Alexandra Neenan, *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress*, Title I, 50 U.S.C. §§4511–4514; Congressional Research Service, R43767, 2024, https://www.congress.gov/crs-product/R43767
[17] Alexandra Neenan, *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress*, Title VII (Voluntary Agreements), 50 U.S.C. §4558; Congressional Research Service, R43767, 2024.
[18] *Defense Production Act: Information Sharing Needed to Improve Use of Authorities*, US Government Accountability Office, GAO-25-107688, June 2025, https://www.gao.gov/assets/gao-25-107688.pdf
[19] Civil Defense Virginia, *A Guide for Developing Continuity of Community Through Community-Based Civil Defense*, n.d., https%3A%2F%2Fcivildefenseradio.com%2Fwp-content%2Fuploads%2F2019%2F02%2FA-Guide-to-A-New-American-Civil-Defense-Structure.pdf&key=sh-0&hmac=017e0e016c7ba6a87a03d837868fd98d0cb380aaae25e81d92a95ea59956b7db.
[20] Abigail E. André, "Modern Disaster Fragmentation," *Fordham Law Review* 3, no. 2 (2024), https://ir.lawnet.fordham.edu/flr/vol93/iss2/7.
[21] Library of Congress, Constitution Annotated, "State Police Power and Tenth Amendment Jurisprudence," https://constitution.congress.gov/browse/essay/amdt10-3-2/ALDE_00013622/.

[22] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.
[23] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.
[24] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[25] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*.
[26] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[27] Shideler and Waller, *Bring Back Civil Defense*.
[28] Dawn Thomas, *Planning for Continuity in the Face of a Cyber-Attack: Challenges and Best Practices*, CNA, 2021.
[29] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*.
[30] Patrick S. Roberts, "The Forgotten Lessons of Civil Defense Federalism for the Homeland Security Era," *Journal of Policy History* 26, no. 3 (2014), https://vtechworks.lib.vt.edu/bitstreams/e040f794-49a6-4dc5-a5e8-8ae0fdcf42e4/download; Shideler and Waller, *Bring Back Civil Defense*.
[31] Roberts, "The Forgotten Lessons of Civil Defense Federalism for the Homeland Security Era."
[32] Kristian Alexander, "Total Defence in Comparative Perspective: Lessons from Finland, Sweden, Switzerland, and Singapore," Institute for Security and Development Policy, 2025, https://www.isdp.eu/total-defence-in-comparative-perspective-lessons-from-finland-sweden-switzerland-and-singapore/; Roberts, "The Forgotten Lessons of Civil Defense Federalism for the Homeland Security Era"; Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[33] Civil Defense Virginia, *Guide to Developing a Community-Based Civil Defense Organization in Your Community*.
[34] CNA, "Civil Defense: From the Cold War to Contemporary Threats."
[35] Dawn Thomas, Braeanna Hillman, Olga Thomas, and Christine Huges, *Civil Defense Considerations for OPNAV at War*, CNA, 2025.
[36] Megan K. McBride, Pamela G. Faber, Kaia Haney, Patricia J. Kannapel, and Samuel Plapinger, *Best Practices for Countering Malign Influence*, CNA, DIM-2025-U-041133-Final, 2025, https://www.cna.org/reports/2025/04/Best-Practices-for-Countering-Malign-Influence.pdf.
[37] Noyes and Humpal, *Why the US Needs a Total Defense Strategy Based on Resilience*.
[38] Dominic Balog-Way, Katherine McComas, and John Besley, "The Evolving Field of Risk Communication," *Risk Analysis* 40, no 1 (2020): 2240–2262. https://pmc.ncbi.nlm.nih.gov/articles/PMC7756860/.
[39] CNA, "Facing 21st-Century Threats: What Every Consequence Manager Should Know."
[40] McBride, Faber, Haney, Kannapel, and Plapinger, *Best Practices for Countering Malign Influence*.
[41] Stapleton and Thomas, *Modern Civil Defense Concept Note*.
[42] Stapleton and Thomas, *Modern Civil Defense Concept Note*.
[43] Shideler and Waller, *Bring Back Civil Defense*.
[44] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[45] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[46] Thomas, *Planning for Continuity in the Face of a Cyber-Attack: Challenges and Best Practices*.
[47] Texas Legislature, S.B. No. 2312, *Chapter 438. Texas Advisory Committee on Geopolitical Conflict*.
[48] Jeffrey Kucik, Jerry Meyerle, John Milton, and Yee San Su, *CNA Maritime Dialogue: US Commercial Ports During a Wartime Mobilization*, CNA, CCP-2025-U-043199-Final, 2025.
[49] Kucik, Meyerle, Milton, and San Su, *CNA Maritime Dialogue*.
[50] Virginia Department of Emergency Management, *Civil Defense: From the Cold War to Contemporary Threats*.
[51] Thomas and Knoll, *21st Century Consequence Management Planning*.
[52] Thomas and Knoll, *21st Century Consequence Management Planning*; Shideler and Waller, *Bring Back Civil Defense*.
[53] Thomas, Hillman, Thomas, and Huges, *Civil Defense Considerations for OPNAV at War*.
[54] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[55] White, Simental, and Holst, *21st Century Homeland Defense & Civil Defense.*
[56] Micheal Lowry, "Hurricane Evacuation Responses: The rules… And the Go Or No-Go Responses" Yale Climate Connections, Oct. 13, 2022, https://yaleclimateconnections.org/2022/10/hurricane-evacuation-responses-the-rules-and-the-go-or-no-go-responses/.

[57] Carson MacPherson-Krusky, "Evacuation Obstacles: Why Some People Remain in Harm's Way During Disasters," Natural Hazards Center, Feb. 18, 2025. https://hazards.colorado.edu/news/research-counts/evacuating-in-disasters-like-hurricane-milton-isnt-simple-there-are-reasons-people-stay-in-harms-way.
[58] Gene Katz, "Insufficient Police Staffing Continues Throughout the US," *American Police Beat Magazine*, 2025, https://apbweb.com/2025/05/insufficient-police-staffing-continues-throughout-the-u-s/.
[59] NEMA, *Empowering Emergency Management to Meet Current and Emerging Threats*, 2023, https://nemaweb.org/wp-content/uploads/2024/04/Empowering-Emergency-Management-to-Meet-Current-Emerging-Threats.pdf.
[60] Verena Gruber and Jonathan Deschênes, "The New Paradigm in Volunteering—And How Nonprofits Can Adapt to 'Neither-Growing-nor-Fading' Brand Relationships," American Marketing Association, July 9, 2024, https://www.ama.org/2024/07/09/the-new-paradigm-in-volunteering-and-how-nonprofits-can-adapt-to-neither-growing-nor-fading-brand-relationships/.
[61] The White House, *National Resilience Strategy*.

This report was written by CNA's Safety and Security Division (SAS).

CNA's Safety and Security Division (SAS) works to help improve decision-making during crisis operations and foster innovative solutions to challenges in the areas of public safety, emergency management, public health preparedness, homeland security, risk management, and national security.

Dedicated to the Safety and Security of the Nation

www.cna.org

About CNA

The CNA Corporation (CNA) is a not-for-profit analytical organization dedicated to the safety and security of the nation. With nearly 700 scientists, analysts, and professional staff across the world, CNA's mission is to provide data-driven, innovative solutions to our nation's toughest problems. It operates the Center for Naval Analyses—the Department of the Navy's federally funded research and development center (FFRDC)—as well as the Institute for Public Research. The Center for Naval Analyses provides objective analytics to inform decision-making by military leaders and ultimately improve the lethality and effectiveness of the joint force. The Institute for Public Research leverages data analytics and innovative methods to support federal, state, and local government officials as they work to advance national and homeland security.

IIM-2026-U-045818-Final