# Transportation Resilience to Areas of Concern

*Requested by*
Hannah Walter, Division of Transportation Planning

**March 21, 2025**

*The Caltrans Division of Research, Innovation and System Information (DRISI) receives and evaluates numerous research problem statements for funding every year. DRISI conducts Preliminary Investigations on these problem statements to better scope and prioritize the proposed research in light of existing credible work on the topics nationally and internationally. Online and print sources for Preliminary Investigations include the National Cooperative Highway Research Program (NCHRP) and other Transportation Research Board (TRB) programs, the American Association of State Highway and Transportation Officials (AASHTO), the research and practices of other transportation agencies, and related academic and industry research. The views and conclusions in cited works, while generally peer reviewed or published by authoritative sources, may not be accepted without qualification by all experts in the field. The contents of this document reflect the views of the authors, who are responsible for the facts and accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the California Department of Transportation, the State of California, or the Federal Highway Administration. This document does not constitute a standard, specification, or regulation. No part of this publication should be construed as an endorsement for a commercial product, manufacturer, contractor, or consultant. Any trade names or photos of commercial products appearing in this publication are for clarity only.*

## Table of Contents

**Executive Summary ..... 3**
Background ..... 3
Summary of Findings ..... 3
Gaps in Findings ..... 8
Next Steps ..... 8
**Detailed Findings ..... 11**
Background ..... 11
Survey of Practice ..... 11
Agencies with Experience Developing Resiliency Strategies ..... 12
Agencies with No Reportable Experience Developing Resiliency Strategies ..... 24
Related Research and Resources ..... 26
**Contacts ..... 40**
**Appendix A: Survey Questions ..... 42**

## List of Abbreviations and Acronyms

| | |
|---|---|
| AASHTO | American Association of State Highway and Transportation Officials |
| BART | Bay Area Rapid Transit (California) |
| Cal OES | California Governor's Office of Emergency Services |
| Caltrans | California Department of Transportation |
| ChatGPT | Chat Generative Pre-Trained Transformer |
| CIP | Critical Infrastructure Protection (U.S. Department of Defense) |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DOT | department of transportation |
| EOP | emergency operations plan |
| FEMA | Federal Emergency Management Agency |
| ICS | incident command structure |
| IP | Internet Protocol |
| IPWG | Infrastructure Protection Working Group (California) |
| IT | information technology |
| ITS | intelligent transportation system |
| MCDA | multicriteria decision analysis |
| MnDOT | Minnesota Department of Transportation |
| MNIT | Minnesota IT Services |
| NRC | Nuclear Regulatory Commission |
| NRG | National Resilience Guidance (FEMA) |
| OT | operational technology |
| PennDOT | Pennsylvania Department of Transportation |
| SAM | State Administrative Manual (California) |
| SEP | State Emergency Plan (California) |
| SLTT | state, local, tribal and territorial |
| SoCalGas | Southern California Gas Company |
| SSA | sector-specific agencies (CISA) |
| STAS | State Threat Assessment System (California) |
| TAM | transportation asset management |
| TL | Technology Letter |
| TS SSP | Transportation Systems Sector-Specific Plan (CISA) |
| UASI | Urban Area Security Initiative |
| USACE | U.S. Army Corps of Engineers |
| WSDOT | Washington State Department of Transportation |

# Executive Summary

## Background

Establishing a resilient transportation system is a primary goal of California Transportation Plan 2050. Resiliency is the ability to withstand or adapt to unplanned events, and to respond to and recover from these events quickly. In addition to the California Department of Transportation's (Caltrans) efforts related to climate resiliency, two additional actions are required to create a resilient transportation system.

First, a broader definition of "critical transportation infrastructure" that extends to the entire California transportation system is needed for resiliency planning. Second, resiliency strategies, including preventive and reactive measures, should be explored to address unplanned events other than climate change that have already occurred or have a high probability of recurring, such as:

- Man-made events and physical attacks (response to, not suppression of, these events), such as explosions, fires and excavations.
- Cyberattacks and technologies (such as artificial intelligence).
- Nuclear blasts.
- Power blackouts or significant power loss.

CTC & Associates surveyed state departments of transportation (DOTs) and other organizations about their approaches to resiliency and preventive and reactive mitigation strategies for the four categories of unplanned events. A literature search supplemented survey findings by examining public agency definitions of critical infrastructure and other resources related to resiliency strategies.

## Summary of Findings

### Survey of Practice

An online survey distributed to state DOT members of the American Association of State Highway and Transportation Officials (AASHTO) Committee on Transportation System Security and Resilience and other contacts identified by the project panel received 11 responses:

**State DOTs**

- Georgia
- Hawaii
- Michigan
- Minnesota (MnDOT)
- Pennsylvania (PennDOT)
- Rhode Island
- Washington (WSDOT)
- Wyoming

**Federal Agency**

- U.S. Army Corps of Engineers (USACE)

**Private Sector Organizations**

- International Motors, LLC (formerly Navistar International Corporation)
- Southern California Gas Company (SoCalGas)

While Hawaii and Georgia DOTs and International Motors reported interest in preparing resiliency strategies for unplanned events, these agencies have not yet done so and have no immediate plans to create them. Hawaii and Georgia DOTs would require resources, staff and best practices to support future efforts. The International Motors respondent needs improved knowledge of suppliers and supply

chain routes. Wyoming DOT has developed resiliency strategies for unplanned events, however, these strategies are not among the specific areas of concern addressed by the survey.

**Resiliency Strategies**

Respondents from seven organizations (*Michigan DOT*, *MnDOT*, *PennDOT*, *Rhode Island DOT, WSDOT*, *USACE* and *SoCalGas*) described efforts to identify locations at risk and collaborate with other entities to develop resiliency strategies for unplanned events in these categories:

- Responses to man-made events and physical attacks.
- Cyberattacks and technologies.
- Nuclear blasts.
- Power blackouts or significant power loss.

*Identifying Locations at Risk*

Respondents described how to identify geographical areas that may be at risk for various threats and offered specific examples:

- *Man-made events and physical attacks*: Potential threat areas and assets include bridges, urban areas, border crossings and military bases.
- *Cyberattacks and technologies*: Agencies consider areas where disruptions to operational technology (OT) networks may impact traveler safety and traffic operations.
- *Nuclear blasts*: DOTs in states with nuclear power plants (*Michigan DOT*, *MnDOT* and *PennDOT*) plan for potential nuclear incidents.
- *Power blackouts or significant power loss:* Areas prone to power losses due to natural events and key transportation buildings or facilities are often the focus for backup generation.

*Collaboration*

State DOTs and SoCalGas work with local, state and federal partners to support transportation network resiliency for a variety of threats. Collaborators are summarized in Table ES1.

**Table ES1. Collaborating Organizations Identified by Respondents**

| Collaborating Entity | State DOT/Other Entity and Description |
|---|---|
| **Federal Agencies** | *Michigan DOT.* National Guard.<br>*Rhode Island DOT*. Federal Highway Administration.<br>*WSDOT*. National Guard, Coast Guard, Cybersecurity and Infrastructure Security Agency (CISA). |
| **State Emergency Management Agencies** | *Michigan DOT*, *MnDOT*, *Rhode Island DOT.*<br>*PennDOT.* DOT staff members are colocated with the state's emergency management agency. |
| **State Information Technology Departments** | *MnDOT*, *PennDOT, Rhode Island DOT.* |
| **Other State Agencies** | *Rhode Island DOT*. Governor's office and Department of Administration.<br>*WSDOT*. Washington State Patrol and Washington Military Department. |

| Collaborating Entity | State DOT/Other Entity and Description |
|---|---|
| **Local Entities** | *Michigan DOT.* Local commissions and agencies.<br>*MnDOT*, *Rhode Island DOT.* |
| **Other Organizations** | *Michigan DOT*. Canadian government, nonprofit and private entities.<br>*SoCalGas.* California public utilities and energy commission, state utilities. |

Respondents described preparedness exercises as a collaboration mechanism, including the following activities conducted in Michigan:

- Simulation of a large, complex attack involving infrastructure and other targets, with federal, state and local partners.
- Working with the U.S. Air National Guard on red team/blue team (attacker/defender) exercises to explore the vulnerabilities of the intelligent transportation system network.
- Statewide exercise simulates a nuclear emergency and response, including evacuation plans, radiation testing, decontamination sites and agricultural concerns.

Emergency response exercises are conducted every other year at Pennsylvania's five nuclear power plants.

*Mitigation Measures*

The preventive and reactive mitigation measures respondents reported in each category of unplanned events are summarized in Table ES2.

**Table ES2. Mitigation Measures by Category of Unplanned Event**

| Category of Unplanned Event | Preventive Mitigation Measure | Reactive Mitigation Measure |
|---|---|---|
| **Man-Made Events and Physical Attacks** | • Identify threats in collaboration with law enforcement and intelligence community (*Michigan DOT*).<br>• Consider trends and emerging concerns when making repairs and updates, and planning for new construction (*Michigan DOT*).<br>• Employ incident tracker software that supports threat management (*MnDOT*).<br>• Colocate with state emergency management officials (*PennDOT*).<br>• Develop methodology for threat-agnostic resilience and stress testing (*USACE*). | • Employ dedicated DOT staff focused on improving mitigation and engaged with emergency management staff at the State Emergency Operations Center (*Michigan DOT*).<br>• Rely on DOT staff who normally performs routine activities to transition to emergency management duties, as needed (*PennDOT*).<br>• Conduct post-disaster response, including debris removal *(USACE*). |

| Category of Unplanned Event | Preventive Mitigation Measure | Reactive Mitigation Measure |
|---|---|---|
| **Cyberattacks and Technologies** | • Provide the central information technology (IT) department with multiple layers of defense by establishing a fully consolidated IT state (*Michigan DOT*).<br>• Establish a dedicated cybersecurity program and partnerships with CISA and the Washington Military Department to support resiliency efforts (*WSDOT*).<br>• Conduct research focused on resilience quantification (*USACE*). | • Employ a cyber event playbook that includes the most likely attacks or compromises (*Michigan DOT*). |
| **Nuclear Blasts** | • Ensure regular participation in drills near Michigan's nuclear power plants to prepare for potential release of nuclear material into the community (*Michigan DOT*).<br>• Establish detour routing and aviation controls, and conduct exercises (*PennDOT*). | • House nuclear response teams in two garages near nuclear plants in partnership with the state environmental agency (*Michigan DOT*).<br>• Make potassium iodide available to staff members and potentially their families in the event of radioactive exposure (*Michigan DOT*). |
| **Significant Power Loss or Blackouts** | • Identify priority areas at risk such as health care and congregate care systems (*Michigan DOT*).<br>• Establish fuel reserves in district facilities (*MnDOT*).<br>• Maintain generator backups at maintenance sheds and district offices (*PennDOT*).<br>• Increase maintenance and testing of backup systems (*WSDOT*).<br>• Establish backup generators at critical facilities (*SoCalGas*). | • Install backup generators in areas that are susceptible to power loss to keep the trunkline and residences free of water during power outages (*Michigan DOT*).<br>• Colocate DOT staff with emergency management agency (*PennDOT*).<br>• Carry out coordination and communication plans (*SoCalGas*).<br>• Ensure a replacement cycle for backup systems (*USACE*). |

## Related Research and Resources

A literature search of publicly available domestic in-progress and published research identified a sampling of publications that are organized into the following topic areas:

- Defining and describing critical infrastructure.
- Research in progress.
- National research.
- Related research.

Resources provided in the first topic area, defining and describing critical infrastructure, are summarized in the following section. Resources from the remaining three categories are summarized in Tables ES3 through ES5, beginning on page 9. Table ES3, Research in Progress, provides the project number and title for research in progress, the research sponsor, a brief project description, and start and expected completion dates for the research effort. Table ES4, National Research, and Table ES5, Related Research,

provide the publication or resource title, the year of publication and a brief description of the resource. More details about each resource can be found in the **Detailed Findings** section of this report.

## Defining and Describing Critical Infrastructure

Caltrans is developing a broader definition of "critical transportation infrastructure" that extends to the entire California transportation system for use in connection with resiliency planning. Definitions and descriptions of critical infrastructure are organized into three categories:

- United States Code.
- Federal agencies.
- California public agencies.

**United States Code.** The definition of critical infrastructure appearing most often in federal agency publications is derived from the text of the USA Patriot Act of 2001, which is reflected in United States Code as 42 U.S. Code § 5195c - Critical infrastructures protection. *From the U.S. Code*:

> **(e) Critical infrastructure defined**
> In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

**Federal Agencies:**

- *U.S. Department of Homeland Security*. Cybersecurity and infrastructure protection are included in the charge of the U.S. Department of Homeland Security. The publication *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* addresses key concepts related to critical infrastructure, including security, resilience, risk and risk management, and partnerships. More recent publications offer tools and guidance for the critical infrastructure community.
- *Cybersecurity and Infrastructure Security Agency.* CISA, an operational component of the U.S. Department of Homeland Security, identifies 16 critical infrastructure sectors. As the CISA website notes, "Of these, four infrastructure sectors — Energy, Communications, Water and Transportation — are critical to the operations of almost all other sectors, as well as each other, and are fundamental to the delivery of the basic societal functions communities seek to provide."

  A CISA publication dedicated to the transportation systems sector addresses seven key subsectors; a companion publication describes a transportation systems sector-specific plan.
- *U.S. Department of Defense.* The U.S. Department of Defense's Protected Critical Infrastructure Program uses the definition of critical infrastructure that appears in the text of the USA Patriot Act of 2001. A category description of critical infrastructure adds text to clarify that the definition applies to "any Federal, State, regional, territorial or local jurisdiction."

**California Public Agencies**:

- *California Governor's Office of Emergency Services (Cal OES).* The definition of critical infrastructure provided by this agency appears to have been informed by the definition appearing in the USA Patriot Act of 2001, which is reflected in United States Code as 42 U.S. Code § 5195c - Critical infrastructures protection.

- CAL OES has established a California Cybersecurity Task Force that supports a Critical Infrastructure Subcommittee, which has identified the following goal related to critical infrastructure:

  > Critical Infrastructure is defined by FEMA [Federal Emergency Management Agency] and Cal OES, but the Critical Infrastructure Subcommittee should take an active role in helping refine those definitions including risk assessment methodologies.

- *California Department of Technology*. Selected resources provide a definition of critical infrastructure and identification of key infrastructure sectors. Chapter 5300, Information Technology — Office of Information Security, of the State Administrative Manual (SAM), includes information security and privacy definitions issued by the California Office of Information Security. The SAM 5300 definitions available on a California Department of Technology website include one for critical infrastructure.

  A June 2018 California Department of Technology publication on recovery and response plans for critical infrastructure presents responses to key questions about California's critical infrastructure and essential functions.

## Gaps in Findings

The survey received a relatively limited response, with 11 total responses and five state DOTs, one federal agency and one private utility company describing resiliency efforts. Of these, respondents offered varying degrees of detail, sometimes quite limited, with regard to current and planned efforts. While an examination of relevant literature indicates current research interest on general resiliency frameworks for state transportation agencies and some focus on cybersecurity, there appears to be limited published research specifically addressing the development of resiliency strategies for the four categories of unplanned events of interest to Caltrans.

## Next Steps

Moving forward, Caltrans could consider:

- Consulting with Michigan DOT's Safety and Security Administration to learn more about:
  - Agency review of resiliency strategies and plans regarding movable bridges, responses to nuclear-involved incidents, emergency funding application improvements, power outages and fuel problems.
  - Development of a cyber event response playbook that will address the most likely attacks or compromises that may impact the organization.
- Engaging with WSDOT to learn more about the agency's dedicated cybersecurity office development of resiliency strategies using security software for converged OT/IT environments in collaboration with the Washington Military Department and CISA.
- Following the activities of the California Cybersecurity Task Force's Critical Infrastructure Subcommittee, under the leadership of Cal OES, as it works to refine definitions of critical infrastructure.
- Examining in detail selected publications cited in this Preliminary Investigation to understand frameworks for resiliency planning and following up when the cited research in progress is complete.

**Table ES3. Research in Progress**

| Project Number and Title | Sponsor | Project Description and Anticipated Period of Performance |
|---|---|---|
| NCHRP Project 20-44(41): Deploying Transportation Resilience Practices in State DOTs: Implementation | National Cooperative Highway Research Program | Planning and facilitating at least four workshops with state DOTs to implement *NCHRP Research Report 970: Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide* (see Table ES4 for this citation).<br>Start date: March 2024; expected completion date: June 2025. |
| Project Number 0-7233: Incorporating Resilience Considerations in Transportation Asset Management Planning and Project Selection Process | Texas Department of Transportation | Producing a framework for resilience-based transportation asset management, including vulnerability assessments for various asset conditions and disruption scenarios. Framework will include a decision-making model for resource allocation that will be tested through pilot studies.<br>Start date: October 2024; expected completion date: August 2026. |
| NCHRP Project 23-32: Transportation Asset Risk and Resilience | National Cooperative Highway Research Program | Providing science-based technical resources to model and quantitatively assess risk and resilience in transportation planning, design, construction, operation and maintenance decisions. Standardized methods will help state DOTs identify the most appropriate risk mitigation or resilience improvement strategies.<br>Start date: November 2023; expected completion date: November 2026. |

**Table ES4. National Research**

| Publication or Resource (Year) | Excerpt from Abstract or Description of Resource |
|---|---|
| National Resilience Guidance: A Collaborative Approach to Building Resilience (2024) | Describes national vision and principles for resilience, including contributing players and systems. Provides methods to strengthen resilience with policy and planning, organizing and engaging stakeholders, financing and prioritization, and evaluation. Presents a Resilience Maturity Model illustrating a community approach to resilience. |
| Cybersecurity Risk Assessment in Connected Intelligent Systems for Designing Resilient Systems (2024) | Explores cyberattack risks to cooperative driving automation (interaction of connected vehicles) through simulations. Develops strategies to enhance cyberattack detection. |
| NCHRP Research Report 1118: Incorporating Resilience into Transportation Networks (2024) | Provides case studies, tools and other materials to support state DOTs in defining and integrating resilience into transportation networks and network planning to avoid and manage potential risks and vulnerabilities caused by unpredictable events. |

| Publication or Resource (Year) | Excerpt from Abstract or Description of Resource |
|---|---|
| NCHRP Web-Only Document 391: Resilience in Transportation Networks, Volume 1: Resilience Case Studies (2024) | Summarizes case studies highlighting frameworks, tools, methods and data needs for increasing the resilience of transportation networks; associated with *NCHRP Research Report 1118*. |
| NCHRP Web-Only Document 391: Resilience in Transportation Networks, Volume 2: Network Resilience Toolkit and Techniques (2024) | Summarizes tools for assessing the resilience of physical infrastructure and institutional arrangements for supporting infrastructure; associated with *NCHRP Research Report 1118*. |
| NCHRP Report 1052: Integrating Resilience Concepts and Strategies into Transportation Planning: A Guide (2023) | Recommends actions for transportation agencies to incorporate resilience into the design and delivery of transportation infrastructure, operations and services. Reviews case studies from Arizona, Colorado, Florida, Georgia, Maryland, Minnesota and Oregon DOTs in addition to Vermont Transportation Agency, California Bay Area Rapid Transit, Texas Capital Area Metropolitan Planning Organization and the Danish Roads Directorate. |
| NCHRP Report 970: Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide (2021) | Presents comprehensive guidance for transportation officials to mainstream resilience concepts into agency decision-making and procedures. Applicable to natural and human-caused threats to transportation systems and services. A 10-step framework and toolkit of supplemental materials covers understanding hazards and determining vulnerabilities, resilience-enhancing actions, communications strategies and other topics. |

**Table ES5. Related Research**

| Publication or Resource (Year) | Excerpt from Abstract or Description of Resource |
|---|---|
| 8R Resilience Model: A Stakeholder-Centered Approach of Disaster Resilience for Transportation Infrastructure and Network (2021) | Develops the 8R Resilience Model based on resilience concepts to assess transportation infrastructure and network resilience from the users' perspective. A multicriteria decision analysis process with the developed model, statistical (survey) model and social media reaction model suggests that adopting the dynamic 8R Resilience Model combined with operational resilience metrics is more beneficial in assessing the criticality of transportation infrastructure than using models developed from survey data and social media reactions. |
| Emergence of Resilience as a Framework for State Departments of Transportation (DOTs) in the United States (2020) | Reviews how state DOTs are confronting a range of risks, including human-caused threats. Covers assessing risk, vulnerability and threats, efforts to incorporate a resilience framework into transportation planning and policy, and other topics. |
| Smart Security?: Evaluating Security Resiliency in the U.S. Department of Transportation's Smart City Challenge (2017) | Explores cities' plans to mitigate and respond to the security risks associated with the integration of technology into transportation systems and transportation system databases. Evaluates the resiliency strategies of Smart City Challenge applicants to respond to security threats. |

# Detailed Findings

## Background

Resiliency goals related to climate action appear in the Caltrans 2020-2024 Strategic Plan and California Transportation Plan 2050. The latter plan also includes the goal of creating a resilient transportation system. Resiliency is the ability to withstand or adapt to unplanned events, and to respond to and recover from these events quickly.

While it has been important for California Department of Transportation (Caltrans) to focus on resiliency related to climate change, two additional actions are required to create a resilient transportation system:

- Defining critical transportation infrastructure in a manner that extends to the entire California transportation system.
- Addressing unplanned events other than climate change that have already occurred or have a high probability of recurring, such as:
    - Man-made events and physical attacks (response to, not suppression of, these events), such as explosions, fires and excavations.
    - Cyberattacks and technologies (such as artificial intelligence).
    - Nuclear blasts.
    - Power blackouts or significant power loss.

This Preliminary Investigation sought the experiences of state departments of transportation (DOTs) and other organizations about approaches to resiliency and mitigation for the four categories of unplanned events identified above. A literature search supplemented survey findings by examining public agency definitions of critical infrastructure and other resources related to resiliency strategies.

## Survey of Practice

An online survey distributed to state DOT members of the American Association of State Highway and Transportation Officials (AASHTO) Committee on Transportation System Security and Resilience gathered information about agency experiences developing resiliency strategies in one or more of the four categories of unplanned events of interest to Caltrans. Representatives from selected federal and state agencies and private sector organizations also received the survey.

Survey questions are provided in Appendix A.

The survey received responses from 11 organizations:

**State DOTs**

- Georgia
- Hawaii
- Michigan
- Minnesota (MnDOT)
- Pennsylvania (PennDOT)
- Rhode Island
- Washington (WSDOT)
- Wyoming

**Federal Agency**

- U.S. Army Corps of Engineers (USACE)

**Private Sector Organizations**

- International Motors, LLC (formerly Navistar International Corporation)
- Southern California Gas Company (SoCalGas)

Survey findings are summarized below in two categories:

- Agencies with experience developing resiliency strategies, which begins immediately below.
- Agencies with no reportable experience developing resiliency strategies, which begins on page 24.

## Agencies with Experience Developing Resiliency Strategies

Respondents from seven agencies reported on experience developing resiliency strategies for one or more of the four unplanned event categories examined in the survey:

**State DOTs**

- Michigan
- MnDOT
- PennDOT
- Rhode Island
- WSDOT

**Federal Agency**

- USACE

**Private Sector Organization**

- SoCalGas

Resiliency strategies are summarized below in four categories of unplanned events:

- Man-made events and physical attacks.
- Cyberattacks and technologies.
- Nuclear blasts.
- Power blackouts or significant power loss.

The summaries that follow examine agency experience in each category in four topic areas: potential geographic locations for incidents, collaboration, preventive measures and reactive mitigation measures. Information was not available for all topic areas; the level of detail in each topic area varies by agency.

### Unplanned Event: Man-Made Events and Physical Attacks

Respondents from the five state DOTs — Michigan DOT, MnDOT, PennDOT, Rhode Island DOT and WSDOT — and USACE described resiliency strategies for the *response* to unplanned man-made events such as explosions, fires and evacuations, or preparations related to strengthening infrastructure rather than preparations to *suppress* such events. These events impacting physical and human assets may target:

- Agency infrastructure, destroying physical assets and operations.
- Agency personnel, resulting in deaths or injuries.

#### Michigan Department of Transportation

Michigan DOT works with other state agencies to manage man-made or physical threats to transportation infrastructure.

| Topic | Description |
|---|---|
| **Potential geographic locations** | The most likely targets include border crossings, Mackinac Bridge, military bases, high-density urban areas and cities that might be targeted by various global ideologies. |

| Topic | Description |
|---|---|
| **Collaboration** | Threats are identified through collaboration with law enforcement and the intelligence community. Michigan DOT's Safety and Security Administration staff members, who also have emergency management responsibilities, are in constant communication with Michigan State Police and emergency responders. Michigan DOT routinely works with the Michigan State Police's Division of Emergency Management and Homeland Security to identify threats. A recent exercise involving a large, complex attack on Michigan infrastructure and other items included federal, state and local partners. |
| **Preventive measures** | Repairs, updates and planning for new construction consider threat trends and emerging concerns. The DOT is transparent with the public regarding updates and repairs. |
| **Reactive mitigation measures** | Partnerships with law enforcement and emergency responders support robust reactive responses to and mitigation of impacts from man-made events. Dedicated DOT staff focuses on mitigation efforts and are colocated with Emergency Management and Homeland Security functions at the State Emergency Operations Center. |

## Michigan DOT's Interest in Resiliency Strategies is "Significant and Continuous"

The Michigan DOT respondent highlighted the role of the agency's Safety and Security Administration, with duties specifically assigned in the areas of emergency management, emergency preparedness and homeland security. Resiliency strategies and plans currently under review address movable bridges, responses to nuclear-involved incidents, emergency funding application improvements, power outages and fuel problems.

**Related Resource:**

**Division of Emergency Management and Homeland Security**, Michigan State Police, 2024.
https://www.michigan.gov/msp/divisions/emhsd
This website provides links to resources, including the Michigan Hazard Mitigation Plan.

### Minnesota Department of Transportation

MnDOT's resiliency efforts in this category of unplanned event focus on workplace violence.

| Topic | Description |
|---|---|
| **Potential geographic locations** | The agency's central office and district headquarters were assessed for vulnerabilities to active aggressors, and some building changes were made. Agencywide assessments have not been completed. |
| **Collaboration** | The agency works with other state agencies on workplace violence. |
| **Preventive measures** | Incident tracker software supports threat management. |
| **Reactive mitigation measures** | Respondent did not address. |

**Related Resource:**

**Critical Infrastructure Protection Program**, Minnesota Department of Public Safety, 2024. https://dps.mn.gov/divisions/hsem/programs/mn-homeland-security/critical-infrastructure-protection-program
The Critical Infrastructure Protection Program, located within the Homeland Security and Emergency Management Division, includes transportation as critical infrastructure. This web page includes links to Cybersecurity and Infrastructure Security Agency (CISA) databases and training on critical infrastructure protection.

### Pennsylvania Department of Transportation

PennDOT has identified multiple potential targets and relies on staff members who routinely perform maintenance activities to seamlessly transition to emergency response.

| Topic | Description |
|---|---|
| **Potential geographic locations** | Numerous bridges and highways have been assumed targets since the September 11, 2001, attacks. Due to the large magnitude of threatened assets, the agency now identifies locational threats in conjunction with specific time frames, such as the movement of presidential motorcades. |
| **Collaboration** | PennDOT fosters a strong connection with the Pennsylvania Emergency Management Agency, which includes colocated DOT staff who provides emergency response when needed. |
| **Preventive measures** | Staff member colocation with Pennsylvania Emergency Management Agency officials supports readiness. |
| **Reactive mitigation measures** | PennDOT staff who normally performs routine activities is relied upon to transition to emergency management roles when necessary. |

### Rhode Island Department of Transportation

The agency's resilience improvement plan is focused on only the climate change implications of sea level rise and flooding from the increased frequency and higher intensity of storms. Locations with the greatest potential for risk of unplanned or physical attack are assessed as part of the agency's continuity of operations plan that addresses potential issues outside of agency control. Rhode Island DOT generally collaborates with the Rhode Island Emergency Management Agency to address unplanned events.

### Washington State Department of Transportation

The agency works with federal and state agencies to assess the risk to many bridges and structures.

| Topic | Description |
|---|---|
| **Potential geographic locations** | Security assessments have been conducted for many bridges and structures. |
| **Collaboration** | The agency collaborates with CISA, U.S. National Guard and Washington State Patrol. |
| **Preventive measures** | This information is considered sensitive and not shared. |

| Topic | Description |
|---|---|
| **Reactive mitigation measures** | Respondent did not address. |

**U.S. Army Corps of Engineers**

While predicting man-made threats is challenging, USACE's ongoing research is supporting risk assessment and resilience.

| Topic | Description |
|---|---|
| **Potential geographic locations** | While natural disaster areas can be identified with high probability, it is more difficult to identify locations in man-made infrastructure. |
| **Collaboration** | The Silver Jackets program (described below) and other USACE programs are designed for interagency collaboration |
| **Preventive measures** | A methodology is being developed for threat-agnostic resilience and stress testing. |
| **Reactive mitigation measures** | The agency is charged with post-disaster response, including debris removal. |

### USACE's Silver Jackets: Interagency Teams Enhance Preparedness

The USACE Silver Jackets are "interagency teams that facilitate collaborative solutions to state, territory or tribe flood risk priorities." Fifty-four intergovernmental flood risk management teams are represented in all states and several territories, bringing together multiple state, federal and sometimes local agencies and tribes "to learn from one another and work together to reduce risk from floods and sometimes other natural hazards. … By applying their shared knowledge, the teams enhance preparedness, mitigation, and response and recovery efforts when such events do occur."

## Unplanned Event: Cyberattacks and Technologies

Respondents described a range of strategic efforts to address threats related to cyberattacks, such as:

- Disruption of port operations (maritime, land and air).
- Freight crane disruptions.
- Rail line disruptions.
- Bridge disruptions.
- Charging station disruptions.
- Commercial vehicle enforcement facility disruptions.
- Delays in project delivery.
- Disruption of traffic lights, tollbooths and electronic signs.
- Blocked access to important files and data, possibly exposing sensitive information.
- Potential for accidents, mass chaos, injuries and loss of life due to disruption of critical infrastructure.

Additionally, respondents considered the anticipated impacts of artificial intelligence technologies, including Metaverse and ChatGPT (Chat Generative Pre-Trained Transformer).

Responses from Michigan DOT and WSDOT are summarized below.

**Michigan Department of Transportation**

Michigan DOT's response focuses on protection of urban areas where disruption of the operational technology (OT) network would have a major impact on safety and operations. The agency's cyber-related activities focus on the "logical vector" rather than the physical location. To increase security of the OT network, the agency is reviewing the intelligent transportation system (ITS) network for older, unpatched devices and unused ports and IP (Internet Protocol) segments.

Attention has been heightened for three significant Michigan bridges that require collaboration with other agencies or organizations to operate, maintain or monitor. While Michigan DOT controls the Blue Water Bridge, as an international crossing, the bridge's physical operations are largely controlled by U.S. Customs and Border Patrol guidance, rules and regulations. The International Bridge and Mackinac Bridge are operated independently.

| Topic | Description |
|---|---|
| **Collaboration** | Working with the U.S. Air National Guard, Michigan DOT has carried out red team/blue team (attacker/defender) exercises to explore the vulnerabilities of the ITS network. The agency has collaborated with local commissions and agencies to protect against business email compromise attacks and provided guidance for safe recovery. Local governments also work to protect Michigan residents by promoting cybersecurity awareness. |
| **Reactive mitigation measures** | While information technology (IT) operations are fully consolidated in the state and the central office has multiple layers of defense, the agency is developing a cyber event response playbook to address the most likely attacks or compromises that may impact the organization. |

**Washington State Department of Transportation**

WSDOT's Strategic Plan, which is being updated, includes a goal for operational resilience — to "support and enhance security for all WSDOT staff and properties, and improve WSDOT's [e]mergency [p]reparedness for response and recovery from natural and man-made incidents (including cyber)." An agency resilience committee is establishing the Operational Technology Cybersecurity Program.

| Topic | Description |
|---|---|
| **Collaboration** | WSDOT has collaborated with the Washington Military Department, the U.S. Coast Guard and CISA on critical infrastructure security assessments. The agency has also started asset discovery — identifying and documenting all assets in the digital ecosystem — in the context of OT. |
| **Reactive mitigation measures** | The agency's dedicated cybersecurity office is developing resiliency strategies using security software for converged OT/IT environments in collaboration with the Washington Military Department and CISA. |

**Related Resources**:

**Strategic Plan**, Washington State Department of Transportation, 2024.
https://wsdot.wa.gov/about/secretary-transportation/strategic-plan
This website notes that resilience, one of the strategic plan's three primary strategic goals, includes a directive to "[p]lan and/or invest resources to improve our ability to mitigate, prepare for and respond to emergencies …."

**Region 10 Fact Sheet**, Region 10 (Alaska, Idaho, Oregon and Washington), Cybersecurity and Infrastructure Security Agency, July 2021.
https://www.cisa.gov/sites/default/files/2024-11/R10_Factsheet_v01.pdf
*From the fact sheet*:

Together with our partners we:

- Support protection, prevent[ion], mitigation, response and recovery efforts for threats and hazards impacting critical infrastructure.
- Guide owners of soft targets and crowded places [to] facilities in improving security and safety protocols.
- Conduct and integrate infrastructure assessments and analysis, including dependencies and cascading effects, on critical infrastructure to influence risk management decisions and investments.
- Facilitate information sharing between public and private sector critical infrastructure partners.
- Enhance election infrastructure security and other critical infrastructure cyber systems.
- Improve situational awareness of cybersecurity risks and incidents.

**Other Public Agency Practices**

In three states, cybersecurity is the responsibility of other state offices:

- Minnesota IT Services (MNIT) coordinates preventive and reactive cyber threat mitigation measures in Minnesota. MnDOT performs additional monitoring on signals to identify geographic locations at risk and participates in a CISA-sponsored collaboration with state, local and private entities.
- In Pennsylvania, the Information Technology program is located in the Commonwealth's Office of Administration. As a result, PennDOT no longer manages day-to-day activities related to cyberattacks but instead coordinates through the statewide effort.
- In Rhode Island, the state's Office of Information Technology and an agency continuity of operations plan address cybersecurity.

USACE is developing a methodology for contested logistics, cybersecurity and resilience, and conducting research on resilience quantification.

## Unplanned Event: Nuclear Blasts

Respondents addressed their agencies' preparedness for the immediate and long-term destructive effects of nuclear emergencies, including potential significant destruction to transportation facilities, other critical infrastructure and humans.

Responses from Michigan DOT, MnDOT and PennDOT are summarized below.

**Michigan Department of Transportation**

Michigan DOT locates garages, resources and personnel outside a 10-mile buffer surrounding the state's operational nuclear power plants. Other locations identified as "natural targets" for nuclear missiles or bombs include major urban populations and military bases throughout the state. As the respondent noted, while resiliency in these areas can't be guaranteed, Michigan DOT's regional approach allows the shifting of assets to accommodate losses in other areas.

| Topic | Description |
|---|---|
| **Collaboration** | The agency is currently participating in the planning and implementation of a statewide exercise simulating a nuclear emergency and response. The exercise is designed to focus on evacuation plans, including radiation testing, decontamination sites and agricultural concerns. Participants will include federal, state, local, nonprofit and private entities, as well as representatives of Canadian provinces. |
| **Reactive mitigation measures** | Michigan DOT regularly participates in drills near Michigan's nuclear power plants to prepare for a potential radiological release. A partnership with Michigan's Department of Environment, Great Lakes and Energy allows for housing response teams in two DOT garages near nuclear sites.<br><br>Within potential blast and fallout areas, Michigan DOT can quickly access potassium iodide for staff members exposed to radioactivity. The agency is working to expand capacity to also supply potassium iodide to staff members' families. |

**Minnesota Department of Transportation**

Minnesota is home to two nuclear power plants. The state's Homeland Security and Emergency Management (HSEM) Division of the Department of Public Safety manages the Radiological Emergency Preparedness program that provides annual training for state agencies and others.

| Topic | Description |
|---|---|
| **Collaboration** | MnDOT engages in response planning for potential incidents at nuclear power plants, including hostile actions, with other state agencies and the HSEM division within the Minnesota DPS. |
| **Reactive mitigation measures** | The state of Minnesota uses a functional annex model of planning, in which the DOT is tasked as a support agency responsible for detailed planning to keep roads open, inspect damaged infrastructure, issue permits and waivers, and other duties in response to an incident. |

**Note**: The respondent described these mitigation measures in terms of nuclear incidents but indicated that these activities are required "no matter what the incident is."

See the citation for *Developing and Maintaining Emergency Operations Plans* below for a discussion of functional annexes.

**Related Resources**:

**Radiological Emergency Preparedness**, Minnesota Department of Public Safety, 2024.
https://dps.mn.gov/divisions/hsem/programs/radiological-emergency-prep
Managed by the Homeland Security and Emergency Management Division, the Radiological Emergency Preparedness program protects public health and safety in the event of a radiological incident at the state's two nuclear power plants. The program includes annual training of state agency employees and others. The program also "conducts emergency plan reviews to make certain state agencies, local jurisdictions and the utility are ready to respond should an incident occur."

**Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101**, Version 2.0, Federal Emergency Management Agency, U.S. Department of Homeland Security, November 2010.
https://www.ready.gov/sites/default/files/2019-06/comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans.pdf
This publication describes the various types of annexes associated with emergency preparedness. The term "annex" is used throughout this guide to "refer to functional, support, hazard/incident-specific or other supplements to the basic plan, consistent with the [National Response Framework]." *From page 3.4 of the guide (page 32 of the PDF)*:

> **Traditional Functional Format**
> The traditional functional structure is probably the most commonly used EOP [emergency operations plan] format. This is the format that many jurisdictions have used to develop EOPs since the 1990s, following FEMA's [Federal Emergency Management Agency's ] Civil Preparedness Guide 1-8 and State and Local Guide 101, which have been rescinded and replaced by this [g]uide. The traditional functional format has three major sections: the basic plan, functional annexes and hazard-specific annexes.
> ….
>
> The functional annexes are individual chapters that focus on missions (e.g., communications, damage assessment). These annexes describe the actions, roles and responsibilities of participating organizations. Functional annexes discuss how the jurisdiction manages the function before, during and after the emergency, and they identify the agencies that implement that function. However, each functional annex addresses only general strategies used for any emergency.
> ….
>
> The traditional format also uses a specific outline to define the elements of each annex. When the format is followed, EOP users can find information in the plan more easily because the same type of information is in the same location. The traditional EOP format is flexible enough to accommodate all jurisdictional strategies. The planning team can add annexes to include a new function or a newly identified hazard or threat. Similarly, the team can separate an operational issue (e.g., mass care) into two separate annexes (e.g., sheltering and feeding, distribution of emergency supplies).

**Pennsylvania Department of Transportation**

Some of Pennsylvania's five active nuclear power plants are located near major cities.

| Topic | Description |
|---|---|
| **Collaboration** | Nuclear power plants are required to conduct emergency response exercises every other year. The exercises involve all impacted state agencies and are coordinated by the Pennsylvania Emergency Management Agency. To cover all five plants, PennDOT participates in three exercises in one year and two the following year. |
| **Reactive mitigation measures** | PennDOT participates in exercises involving detour routing and aviation controls. The respondent noted that the only significant nuclear incident in the U.S. was in the 1970s, 15 miles from the Pennsylvania state capital (see the **Note** below). |

**Note:** The U.S. Nuclear Regulatory Commission's (NRC's) "Backgrounder on the Three Mile Island Accident" provides information about an incident at the Three Mile Island nuclear facility, which the PennDOT respondent alluded to above:

> The Three Mile Island Unit 2 [TMI-2] reactor, near Middletown, Pa., partially melted down on March 28, 1979. This was the most serious accident in U.S. commercial nuclear power plant operating history, although its small radioactive releases had no detectable health effects on plant workers or the public. Its aftermath brought about sweeping changes involving emergency response planning, reactor operator training, human factors engineering, radiation protection and many other areas of nuclear power plant operations. It also caused the NRC to tighten and heighten its regulatory oversight. All of these changes significantly enhanced U.S. reactor safety.
>
> A combination of equipment malfunctions, design-related problems and worker errors led to TMI-2's partial meltdown and very small off-site releases of radioactivity.

## Unplanned Event: Power Blackouts or Significant Power Loss

Power blackouts or significant power loss may be caused by technical failure, electrical grid sabotage or attacks such as high-altitude electromagnetic pulse that may result in:

- Widespread and prolonged power blackouts paralyzing transportation facilities, the State Highway System and its operations.
- Severe backups, crashes and fatalities.
- Long fuel lines or out-of-service gas stations that make it difficult to obtain gas for generators.

Given this backdrop, survey respondents described efforts to identify geographic locations that may be at higher risk of power interruption, collaborative efforts to support resiliency against threats of power outages, and preventive and reactive mitigation measures to address power loss. Survey responses regarding resiliency efforts in the context of power blackouts are summarized in Table 1.

**Table 1. Agency Response to Threat of Power Blackouts or Significant Power Loss**

| State DOT/ Other Entity | Identification of Likely Geographic Locations | Collaboration | Preventive Mitigation Measure | Reactive Mitigation Measure |
|---|---|---|---|---|
| **Michigan DOT** | • Working to remedy and build resiliency against recurring power losses over one large area due to natural events.<br>• In other areas within the energy sector, will identify geographical and mechanical weaknesses. | • Working with state and federal partners to strengthen areas at risk.<br>• Participating in exercises with Canadian and domestic federal, state and local partners. | • Identifying areas of risk.<br>• Prioritizing power needs (e.g., health care and congregate care systems) | Installing backup generators in areas identified as susceptible to power loss that are also prone to flooding, which has inundated some highway areas and residents' homes with water and sewage. |
| **MnDOT** | Ensures at least one larger/primary building in each district has a backup generator. | No collaboration | Have fuel reserves in districts with known capacity. | Respondent did not address. |
| **PennDOT** | Not attempted | Colocates with emergency management agency, allowing DOT to respond immediately when needed. | No measures other than some generator backups at maintenance sheds and district offices. | Interact directly with staff members who are colocated with the emergency management agency. |
| **Rhode Island DOT** | Not attempted | State emergency management agency | Respondent did not address. | Respondent did not address. |
| **WSDOT** | Key facilities | No collaboration | Increase maintenance and testing of backup systems. | Created replacement cycle for backup systems |
| **USACE** | Considers the methodological aspects of energy resilience as part of critical infrastructure | Seeks collaboration in areas surrounding military installations. | Respondent did not address. | Respondent did not address. |
| **SoCalGas** | Compressor stations and critical facilities | Collaborates with California Public Utilities Commission, California Energy Commission and other state utilities. | • Provide backup generators at compressor stations and critical facilities.<br>• Build in gas system redundancies. | Has developed plans for coordination and communication. |

## Assessing Resiliency Strategy Development

Respondents assessed their agencies' efforts to develop resiliency strategies to unplanned events in the following topic areas:

- Benefits of organizational resiliency efforts.
- Challenges encountered in resiliency strategy development.
- Best practices for preparing for or responding to unplanned events.

### Benefits of Organizational Resiliency Efforts

In addition to the assessment that resiliency strategy planning results in less risk of disaster (*SoCalGas*), survey respondents reported a variety of transportation infrastructure, public and agency employee benefits.

**Transportation Infrastructure Benefits**

- Developing strategic efforts reduces response time and impacts of unplanned events (*MnDOT*).
- Identifying areas of susceptibility may help eliminate threats and support an infrastructure better able to respond to emergencies (*Michigan DOT*).
- Improving resiliency can lead to substantial cost savings related to emergency response (*USACE*).

**Public Benefits**

- Strategic planning for resiliency can help ensure continuity of services (*Michigan DOT, MnDOT*).

**Agency Employee Benefits**

- An agencywide strategic goal creates a culture of resiliency across all staff (*WSDOT*).
- Helping communities during emergencies is a morale booster for employees (*Michigan DOT*).
- Knowledge and practice of how to respond to emergencies reduce staff confusion and the potential impact of unforeseen incidents (*PennDOT*).
- Resiliency strategies can support continued employment during emergencies *(Michigan DOT*).

### Challenges Encountered in Resiliency Strategy Development

For MnDOT and SoCalGas, funding and resources are the primary challenges associated with resiliency planning. Investment financing is an issue for Michigan DOT, which required a grant to purchase a generator for an area that has experienced power loss and flooding. At WSDOT, resources are "by far the greatest limiting factor," and the agency has been unsuccessful in securing funding from the state legislature for resiliency efforts.

Other challenges:

- Clear guidance on best practices is lacking (*SoCalGas*).
- Multiagency collaboration can be time-consuming (*Rhode Island DOT*).
- Time and approvals for strategy efforts can be hard to secure (*MnDOT*), including extra effort for subject matter experts to bring a new administration up to speed on existing methodologies and response plans (*PennDOT*).

The SoCalGas respondent highlighted the need to focus on current risks. The USACE respondent noted that stakeholders may confuse risk (a product of threat, vulnerability and consequence) with resilience

(the ability to recover and adapt). Some activities that may be considered resilience-related are actually traditional risk management methods and not applicable to unplanned events.

**Best Practices for Preparing for or Responding to Unplanned Events**

Lessons learned or best practices for other agencies to consider when developing resiliency strategies are summarized below in three topic areas:

- Partnerships and collaboration.
- Employee expertise and management structure.
- Planning and resources.

**Partnerships and collaboration.** Working with similar agencies and community-based organizations to understand potential impacts on customers, and communicating and coordinating with other government agencies can support organizational efforts to create resilience to unplanned events (*SoCalGas*).

Investing in relationships with community and agency partners can help identify weaknesses or other issues to be addressed (*Michigan DOT*). Creating workgroups with champions at the executive level can be beneficial (*WSDOT*).

**Employee expertise and management structure.** Leveraging the range of talents and expertise in an agency and embracing a variety of perspectives can result in more robust responses to unplanned events (*Michigan DOT*, *PennDOT*).

An ICS with clear overall management responsibilities within an organization can result in better communication, coordination and priority-setting. The ICS need not be rigid but should clearly identify resources, contacts and functions within the agency (*PennDOT*).

**Planning and resources.** Respondents offered programmatic or funding recommendations for supporting resiliency to unplanned events:

- Employ tabletop exercises to help identify resiliency opportunities and strategies (*MnDOT*).
- Ensure adequate organizational capacity for remote work to support flexibility for resilience (*MnDOT*).
- Prioritize needs to act quickly when funding opportunities arise and leverage as many grant opportunities as possible (*WSDOT*).
- Undertake appropriate planning to be prepared to deliver a quick response to emergencies and disasters (*Michigan DOT*).
- Analyze risk management and resilience separately but implement in tandem. Resilience should be quantifiable and resilience-related data should be part of the policy-making process (*USACE*).

Two publications on resilience co-authored by the USACE respondent highlight the role of science in resilience:

> **"The Role of Science in Resilience Planning for Military-Civilian Domains in the U.S. and NATO,"** *Defence Studies*, Vol. 24, Issue 4, pages 493-524, June 2024. https://doi.org/10.1080/14702436.2024.2365218
> *From the abstract*: In recent years, the NATO member nations have committed to a coordinated approach to strengthening resilience among the Allies, including the development of National

Resilience Plans (NRPs). The Allies outlined the extent to which the robustness of their respective military capacities requires the designed resilience of systems that bridge civilian and military domains. This article outlines the role that resilience plays in supporting tactical and strategic measures of national security and defense within military and civilian domains. This exploration provides an outline of how resilience is currently applied in practice by the U.S. Department of Defense (DOD) and NATO. Building on this diversity of applications, various categorical forms of resilience drawn from the empirical science of resilience are positioned within NATO's emerging frame for "layered" resilience. This article reinforces the scientific debate that an optimal orientation to resilience leaves open the door for the transformative adaptation of function and identity when the single-equilibrium processes of resilience reach their limits. This article concludes with a normative perspective on how military and civilian resilience planning could support the development of NRPs that would amplify the Allies' collective capacity to face shared security threats.

**"The Science and Practice of Resilience,"** *Risk, Systems and Decisions*, Igor Linkov and Benjamin Trump, Springer Cham, 2019.
Publisher description at https://link.springer.com/book/10.1007/978-3-030-04565-4
*From the publisher description:* This book offers a comprehensive view on resilience based upon state-of-the-science theories and methodological applications that resilience may fill. Specifically, this text provides a compendium of knowledge on the theory, methods and practice of resilience across a variety of country and case contexts, and demonstrates how a resilience-based approach can help further improved infrastructure, vibrant societies, and sustainable environments and ecologies, among many others.

## Agencies with No Reportable Experience Developing Resiliency Strategies

Respondents from Georgia DOT, Hawaii DOT and International Motors, LLC reported that their agencies have interest in preparing resiliency strategies for unplanned events but have not yet done so and have no immediate plans. Wyoming DOT has not yet developed resiliency strategies for the unplanned events of interest to Caltrans. Summarized below are these agency responses.

**Georgia DOT**. The agency has a plan for continuity of operations, succession and "special operations" but no resiliency strategies specific to unplanned events. Staff time, best practices and templates would support efforts to develop resiliency strategies for unplanned events.

**Hawaii DOT**. The agency has developed a Hazard Viewer, which covers natural disasters and locations of assets; a Climate Adaptation Action Plan, published in 2021; and a climate mitigation plan in process. To act on interest in developing a cyberattack policy, the agency requires more resources, staff and data transparency. The respondent noted that teamwork is needed at all levels to help achieve resilient and vibrant communities. See *Related Resources* below for further details.

*Related Resources*:

**Resilience Hazard Viewer: HDOT Asset and Hazard Assessment**, Hawaii Department of Transportation, 2024.
https://hidot.hawaii.gov/resilience/
This website presents an interactive map that identifies bridges, culverts, tunnels and roadways, and provides risk or impacts from several natural events, including landslides, sea level rise, tsunami, lava flow and wildfire.

**Hawaii Highways Climate Adaptation Action Plan: Strategies for a More Resilient Future**, Hawaii Department of Transportation, May 2021.
https://hidot.hawaii.gov/wp-content/uploads/2021/07/HDOT-Climate-Resilience-Action-Plan-and-Appendices-May-2021.pdf
*From the background:* The [a]ction [p]lan provides a roadmap for HDOT's (Hawaii DOT's] Highways Division to make the highway system more resilient to climate-related effects. It presents an exposure assessment of climate hazards to the [s]tate's highways based on both historical and future climate condition research and data. The [a]ction [p]lan prioritizes recommendations in a multi-year [i]mplementation [p]lan that encompasses all aspects of HDOT's core functions and programs — funding, planning, designing, constructing, operating, maintaining and protecting highway assets. It is considered a living document and will be revised as needed to reflect changes in conditions and implementation status.

**Wyoming DOT**. While Wyoming DOT has developed resiliency strategies for unplanned events, these events are not among the four categories of unplanned events addressed in the survey. The agency is currently developing a risk and resilience plan for natural events only. The respondent noted that uncertainties regarding where, when and how unplanned events may unfold make strategy choices challenging. However, developing resiliency strategies results in effective solutions for more durable transportation facilities and can inspire public trust.

**International Motors, LLC**. The agency requires full knowledge of suppliers and supply chain routes to develop resilient logistics for supply chain issues.

# Related Research and Resources

A literature search of publicly available domestic in-progress and published research identified publications that are organized into the following topic areas:

- Defining and describing critical infrastructure.
- Research in progress.
- National research.
- Related research.

## Defining and Describing Critical Infrastructure

Caltrans is developing a broader definition of "critical transportation infrastructure" that extends to the entire California transportation system for use in connection with resiliency planning. Definitions and descriptions of critical infrastructure are presented below in three categories:

- United States Code.
- Federal agencies.
- California public agencies.

### United States Code

The definition of critical infrastructure appearing most often in federal agency publications is derived from the text of the USA Patriot Act of 2001, which is reflected in United States Code as 42 U.S. Code § 5195c - Critical infrastructures protection.

**42 U.S. Code § 5195c - Critical infrastructures protection**, Title 42, The Public Health and Welfare, United States Code, 2023.
*Source*: §1016(e) of the USA Patriot Act of 2001
https://www.govinfo.gov/content/pkg/USCODE-2023-title42/pdf/USCODE-2023-title42-chap68-subchapIV-B-sec5195c.pdf
*From the code*:

> **(e) Critical infrastructure defined**
> In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

### Federal Agencies

Highlighted below are definitions and descriptions of critical infrastructure used by selected federal agencies:

- U.S. Department of Homeland Security.
- CISA.
- U.S. Department of Defense.

#### U.S. Department of Homeland Security

Cybersecurity and infrastructure protection are included in the charge of the U.S. Department of Homeland Security. The 2013 plan cited below addresses key concepts related to critical infrastructure,

including security, resilience, risk and risk management, and partnerships. More recent publications offer tools and guidance for the "critical infrastructure community."

**National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience**, U.S. Department of Homeland Security, 2013.
https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf
Chapter 3, Critical Infrastructure Environment, which begins on page 7 of the plan (page 13 of the PDF), addresses the following key concepts:

> **Key Concepts**
> The key concepts described below provide context for this critical infrastructure environment. An understanding of these key concepts influences the state of critical infrastructure and shapes the community's approach to ensuring security and resilience.
>
> - **Critical infrastructure** represents "systems and assets, whether physical or virtual, so vital to the United States that the in capacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The National Plan acknowledges that the [n]ation's critical infrastructure is largely owned and operated by the private sector; however, [f]ederal and SLTT [state, local, tribal and territorial] governments also own and operate critical infrastructure, as do foreign entities and companies.
> - PPD-21 [Presidential Policy Directive 21] defines **security** as "reducing the risk to critical infrastructure by physical means or defens[ive] cyber measures to intrusions, attacks, or the effects of natural or man-made disasters." There are several elements of securing critical infrastructure systems, including addressing threats and vulnerabilities and sharing accurate information and analysis on current and future risks. Prevention and protection activities contribute to strengthening critical infrastructure security.
> - **Resilience**, as defined in PPD-21, is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions ... [it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.
> - Security and resilience are strengthened through risk management. **Risk** refers to the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences;" **risk management** is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost."
> - **Partnerships** enable more effective and efficient risk management. Within the context of this National Plan, a partnership is defined as close cooperation between parties having common interests in achieving a shared vision. For the critical infrastructure community, leadership involvement, open communication, and trusted relationships are essential elements to partnership.

The plan also provides a glossary and of terms, including several related to critical infrastructure.

*Related Resources*:

**Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach**, U.S. Department of Homeland Security, December 2020.
https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf
*From page 1 of the document (page 2 of the PDF)*: Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. It is influenced by the nature and magnitude of a threat or hazard, the vulnerabilities from that threat or hazard, and the consequences that could result. Risk information allows partners, from facility owners and operators to [f]ederal agencies, to prioritize risk management efforts.

This supplement describes a useful critical infrastructure risk management approach, which supports the risk management framework depicted in Figure 1. The framework enables the integration of strategies, capabilities, and governance structures to enable risk-informed decision making related to the [n]ation's critical infrastructure. The critical infrastructure risk management approach described in this supplement can be applied to all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and acts of terrorism, although different information and methodologies may be used to understand each.

**Critical Infrastructure Threat Information Sharing Framework: A Reference Guide for the Critical Infrastructure Community**, U.S. Department of Homeland Security, October 2016.
https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf
*From the executive summary:* This Framework is a resource to help critical infrastructure owners and operators, as well as other private sector, [f]ederal, and [s]tate, local, tribal, and territorial (SLTT) government partners that share threat information, learn where they can turn, and in what circumstances, to both receive and report threat information. Threat information in this Framework is limited to information sharing pertaining to man-made threats, including both cyber and physical threats, to critical infrastructure.

**Cybersecurity and Infrastructure Security Agency**

CISA, an operational component of the U.S. Department of Homeland Security, identifies 16 "critical infrastructure sectors." As the CISA website notes, "Of these, four infrastructure sectors — Energy, Communications, Water and Transportation — are critical to the operations of almost all other sectors, as well as each other, and are fundamental to the delivery of the basic societal functions communities seek to provide."

Highlighted below are selected portions of the CISA website and CISA plans related to critical infrastructure.

**Critical Infrastructure Security and Resilience**, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, undated.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
*From the website:*

> **Overview**
> *Critical Infrastructure* [is] those assets, systems and networks that provide functions necessary for our way of life. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences.

**Critical Infrastructure Systems**, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, undated.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems
*From the website*:

> There are 16 critical infrastructure sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

**Critical Infrastructure Sectors**, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, undated.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
This website identifies and describes CISA's 16 critical infrastructure sectors:

- Chemical.
- Commercial Facilities.
- Communications.
- Critical manufacturing.
- Dams.
- Defense industrial base.
- Emergency services.
- Energy.
- Financial services.
- Food and agriculture.
- Government services and facilities.
- Healthcare and public health.
- Information technology.
- Nuclear reactors, materials, and waste.
- Transportation systems.
- Water and wastewater.

**Transportation Systems Sector**, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, undated.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector
*From the website*:

> **Sector Details**
> The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. The nation's transportation system quickly, safely and securely moves people and goods through the country and overseas.

**Overview**

The Transportation Systems Sector consists of seven key subsectors, or modes:

- **Aviation** includes aircraft, air traffic control systems, and about 19,700 airports, heliports and landing strips. Approximately 500 provide commercial aviation services at civil and joint-use military airports, heliports and sea plane bases. In addition, the aviation mode includes commercial and recreational aircraft (manned and unmanned) and a wide variety of support services, such as aircraft repair stations, fueling facilities, navigation aids and flight schools.
- **Highway and Motor Carrier** encompasses more than 4 million miles of roadway, more than 600,000 bridges and more than 350 tunnels. Vehicles include trucks, including those carrying hazardous materials; other commercial vehicles, including commercial motor coaches and school buses; vehicle and driver licensing systems; traffic management systems; and cyber systems used for operational management.
- **Maritime Transportation System** consists of about 95,000 miles of coastline, 361 ports, more than 25,000 miles of waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from and on the water.
- **Mass Transit and Passenger Rail** includes terminals, operational systems and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, heavy rail — also known as subways or metros — light rail, passenger rail and vanpool/rideshare. Public transportation and passenger rail operations provided an estimated 10.8 billion passenger trips in 2014.
- **Pipeline Systems** consist of more than 2.5 million miles of pipelines spanning the country and carrying nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. Above-ground assets, such as compressor stations and pumping stations, are also included. [***Note***: In California, the California Energy Commission is the state agency responsible for this infrastructure, as per the State Emergency Plan (SEP) and California Emergency Support Function 12 Utilities Annex to the SEP, among other state codes.]
- **Freight Rail** consists of seven major carriers, hundreds of smaller railroads, over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives. An estimated 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.
- **Postal and Shipping** moves about 720 million letters and packages each day and includes large integrated carriers, regional and local courier services, mail services, mail management firms, and chartered and delivery services.

**Sector-Specific Plan**

The Transportation Systems Sector-Specific Plan [see *Related Resource* below for the citation] details how the National Infrastructure Protection Plan risk management framework [see **Related Research and Resources**, page 27, for the citation] is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector Risk Management Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Postal and Shipping Sector was consolidated within the Transportation Systems Sector in 2013 under Presidential Policy Directive 21. The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

*Related Resource:*

**Transportation Systems Sector-Specific Plan,** Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, 2015.
https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf
*From the preface*: The TS SSP [Transportation Systems Sector-Specific Plan] is a planning tool for the SSAs [sector-specific agencies], critical infrastructure owners and operators, and partners at the regional, [s]tate, local, tribal and territorial levels. The TS SSP guides and integrates efforts to secure and strengthen the resilience of critical infrastructure, identifies the [s]ector's security and resilience priorities, and describes the approach to managing critical infrastructure risk. It builds upon the 2010 TS SSP and aligns with other national strategies and plans that address preparedness to prevent, protect against, mitigate, respond to, and recover from man-made and natural hazards. The TS SSP is intended to focus the resources and programming of agencies and companies on collaboratively determined priorities for effective management of sector risks. It is not intended to replace agency- or company-specific planning documents or risk management processes.

**Department of Defense**

The U.S. Department of Defense's Protected Critical Infrastructure Program uses the definition of critical infrastructure that appears in the text of the USA Patriot Act of 2001. A category description of critical infrastructure adds text to clarify that the definition applies to "any [f]ederal, [s]tate, regional, territorial or local jurisdiction."

**DoD Protected Critical Infrastructure Program**, Assistant Secretary of Defense for Homeland Defense and Global Security, Office of the Under Secretary of Defense for Policy, U.S. Department of Defense, undated.
https://policy.defense.gov/OUSDP-Offices/ASD-HDGS/Defense-Critical-Infrastructure-Program/
*From the website:*

**What is Critical Infrastructure?**
Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

**What is CIP?**
Critical Infrastructure Protection (CIP) consists of actions taken to prevent, remediate or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.

**General Critical Infrastructure Information**, Department of Defense Controlled Unclassified Information Program, U.S. Department of Defense, undated.
https://www.dodcui.mil/Critical-Infrastructure/General-Critical-Infrastructure-Information/
*From the website*:

**Category Description:**
Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any [f]ederal, [s]tate, regional, territorial or local jurisdiction.

## California Public Agencies

Online resources and publications associated with critical infrastructure are highlighted below from two California public agencies:

- California Governor's Office of Emergency Services (Cal OES).
- California Department of Technology.

### California Governor's Office of Emergency Services

The definition of critical infrastructure provided by Cal OES appears to have been informed by the definition appearing in the USA Patriot Act of 2001, which is reflected in United States Code as 42 U.S. Code § 5195c - Critical infrastructures protection.

Presented below are selected portions of the Cal OES website.

**Critical Infrastructure Protection**, California Governor's Office of Emergency Services, 2025.
https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/state-threat-assessment-center/critical-infrastructure-protection/
*From the website:*

> Critical infrastructure is the assets, systems and networks, whether physical or virtual, so vital to California that their incapacitation or destruction would have a debilitating effect on security, economic security, public health or safety, or any combination of these.
>
> Protecting California's critical infrastructure is a vital component to the overall strategy to protect California and its citizens. Cal OES recognizes that California society and way of life are dependent on a reliable network of infrastructure.

Cal OES efforts associated with critical infrastructure:

> **Infrastructure Protection Working Group (IPWG)**, California Governor's Office of Emergency Services, 2025.
> https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/state-threat-assessment-center/critical-infrastructure-protection/outreach-and-coordination-projects-programs/
> *From the website:* The Infrastructure Protection Working Group (IPWG) brings together homeland security partners and programs within the state to help collectively address threats and hazards to critical infrastructure.
>
> The IPWG membership comes from the State Threat Assessment System (STAS) Critical Infrastructure Protection or Risk Management Units, Urban Area Security Initiative (UASI) representatives, emergency management organizations, and security staff from county and local offices throughout the state.
>
> The working group meets quarterly and upon request by a member to address a specific threat or hazard.

**California Cybersecurity Task Force**, California Governor's Office of Emergency Services, 2025.
https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/cybersecurity-task-force/
Seven subcommittees within this task force focus on specific strategic goals. Goals of the Critical Infrastructure Subcommittee:

- Provide recommendations for cybersecurity protection, prevention, detection and response for critical infrastructure in the [s]tate.
- Critical Infrastructure is defined by FEMA and Cal OES, but the Critical Infrastructure Subcommittee should take an active role in helping refine those definitions, including risk assessment methodologies.
- Provide a forum for advising the California Cybersecurity Integration Center on critical infrastructure issues related to state and federal legislation and regulatory frameworks/proposals, and to facilitate outreach required by these statutes and regulations.

## California Department of Technology

The California Department of Technology resources below provide a definition of critical infrastructure and identification of key infrastructure sectors, and offer responses to key questions about California's critical infrastructure and essential functions.

**SAM 5300 Definitions**, California Department of Technology, 2025.
https://cdt.ca.gov/security/technical-definitions/#C
Chapter 5300, Information Technology — Office of Information Security, of the State Administrative Manual (SAM) includes information security and privacy definitions issued by the California Office of Information Security. The SAM 5300 definitions available on this California Department of Technology web page include one for critical infrastructure.

Click on "C" to expand that segment of the definitions and scroll down to "critical infrastructure." *From the website*:

**SAM 5300 Definitions**

**C >> Critical Infrastructure**
Critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation['s] and state's economy, security and health.

Assets [are] identified as essential to the state, U.S. society and the economy, public health, safety, economic security or any combination thereof. These include, as examples, facilities, systems and services within the following sectors:

1. Chemical.
2. Commercial Facilities.
3. Communications (telecommunications).
4. Critical Manufacturing.
5. Dams and [T]heir [C]ontrol [S]ystems.
6. Defense Industrial Base (police, military).
7. Emergency Services (first responders, police, military).
8. Energy [electricity generation, transmission and distribution; gas production, transport and distribution; and oil and oil products production, transport and distribution; heating (e.g., natural gas, fuel oil, district heating)].

9. Financial Services (banking, clearing).
10. Food and Agriculture (agriculture, food production and distribution).
11. Government Facilities.
12. Healthcare and Public Health (hospitals, ambulances).
13. Information Technology.
14. Nuclear Reactors, Materials and Waste.
15. Transportation Systems (fuel supply, railway network, airports, ports, harbors, inland shipping).
16. Water and Wastewater Systems [water supply, drinking water, waste water/sewage, stemming of surface water (e.g., dikes and sluices)].

*Sources*: U.S. Department of Homeland Security and Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e).

**Recovery and Response Plans for Critical Infrastructure: Frequently Asked Questions**, Technology Letter (TL) 18-03, California Department of Technology, June 2018.
https://cdt.ca.gov/wp-content/uploads/2018/06/FAQ-Critical-Infrastructure_04-06-2018.pdf
This question-and-answer publication addresses these questions related to critical infrastructure:

- What is the process to identify critical infrastructure, consistent with SAM 5300.4?
- What criteria should be considered for identifying critical infrastructure?
- What are California State Essential Functions?
- Are there any guiding documents or supporting directives on [the] critical infrastructure initiative?
- Are there specific examples of critical infrastructure?
- Are there any additional resources available?

## Research in Progress

**NCHRP Project 20-44(41): Deploying Transportation Resilience Practices in State DOTs: Implementation**, start date: March 2024; expected completion date: June 2025.
Project description at https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=5184

**Note**: See **Related Research and Resources**, page 37, for the citation for *NCHRP Research Report 970*, the completed project associated with this project in process.

*From the objective:* The objective of this project is to develop workshops to support state DOTs in implementing *NCHRP Research Report 970: Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide* through the planning and facilitation of at least four pilot workshops with state DOTs. The workshops would cover the concepts underlying the guide and will allow different state DOT staff to assess their current resilience status and to identify state DOT-specific strategies.

**Project Number 0-7233: Incorporating Resilience Considerations in Transportation Asset Management Planning and Project Selection Process**, Texas Department of Transportation, start date: October 2024; expected completion date: August 2026.
Project description at https://library.ctr.utexas.edu/Presto/project=0-7233
*From the project description:* This project aims to advance resilience-based transportation asset management (TAM) planning and project selection through the systematic integration of resilience for various assets. It encompasses five primary tasks: (1) Collecting asset and hazard datasets and integrating those diverse datasets for accurate disruption scenario analysis and asset condition assessment. (2) Performing vulnerability assessment based on asset conditions and disruption scenario

analysis. (3) Developing a resilience-based TAM framework for various assets, which involves synthesizing insights from [a] literature review and interviews with the Resilience Working Group to (i) identify resilience metrics for different asset types, (ii) conduct life cycle cost analysis, (iii) develop a decision-making model for resource allocation, and (iv) [conduct] sensitivity analysis to identify critical factors for improving resilience and investment prioritization. (4) Creating a user-friendly tool to operationalize the proposed framework. (5) Conducting pilot studies to demonstrate the resilience-based TAM framework. This project benefits district transportation authorities by improving resource allocation, asset resilience, and project selection. Through structured evaluation of trade-offs between competing TAM objectives like resilience and cost-effectiveness, and investment prioritization, this project ensures efficient resource allocation and long-term resilience under resource constraints. Ultimately, this project establishes the groundwork for the resilience-based TAM Plan and Statewide Resiliency Plan.

**NCHRP Project 23-32: Transportation Asset Risk and Resilience**, start date: November 2023; expected completion date: November 2026.
Project description at https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=5361
*From the background:* Investing in risk and resilience strategies and recovery planning to reduce or eliminate the impact of external events is paramount to ensuring a thriving and viable transportation system. Risk management requires (1) identifying and assessing potential threats and hazards, (2) identifying asset vulnerabilities from applicable threats, (3) evaluating potential mitigation actions to reduce risk, (4) a clear and easy implementation process to prioritize mitigation activities, and (5) investments that align with agency strategic and performance goals. Although many research efforts have been conducted on asset and performance management, information on analytical methods to support risk-based asset management throughout the life cycle of the system, from inception to operation, is lagging. In addition, an understanding of the relationship between risks and system resilience is lacking.
….

The objective of this research is to provide a science-based technical resource to assess risk and resilience in transportation planning, design, construction, operation and maintenance decisions. At a minimum, the research shall develop:

- Quantitative, repeatable methods for conducting risk assessments on top priority threats/hazards for transportation assets;
- A historical data-capture process and system to support risk and resilience modeling and assessments;
- Quantitative resilience assessment methods and metrics for transportation assets; and
- Standardized methods to help state DOTs and other transportation agencies identify the most appropriate risk mitigation or resilience improvement strategies.

## National Research

**National Resilience Guidance: A Collaborative Approach to Building Resilience**, Federal Emergency Management Agency, August 2024.
https://www.fema.gov/sites/default/files/documents/fema_national-resilience-guidance_august2024.pdf
*From the scope and audience*: The NRG [National Resilience Guidance] is intended to help all individuals, communities and organizations understand our nation's vision for resilience, the key principles that must be applied to strengthen resilience, and the players and systems that contribute to resilience. It

also outlines how to strengthen resilience by organizing and engaging people, incorporating resilience concepts into planning efforts, creating change through policies, prioritizing projects and programs, financing resilience efforts, and measuring and evaluating resilience. Finally, the NRG includes a Resilience Maturity Model that illustrates stages in the evolution of a community's approach to resilience.

**Cybersecurity Risk Assessment in Connected Intelligent Systems for Designing Resilient Systems**, Zulqarnain Khattak, Sean Qian and Gavin Lin, U.S. Department of Transportation, Safety21 University Transportation Center, July 2024.
Publication available at https://rosap.ntl.bts.gov/view/dot/77498
*From the report's conclusion*:

> This research developed a framework to study cyberattack simulation and anomaly detection within cooperative driving automation. The study utilized real-world data from field experiments of cooperative driving automation to simulate cyberattacks and perform anomaly detection. The study simulates [s]poofing, [m]essage [f]alsification and [r]eplay attacks based on three anomalies (short, bias and gradual drift) to capture complex attack patterns and employs long short-term memory neural network with Gaussian mixture model for anomaly detection, ensuring resilient operation of cooperative driving. Our aggregation strategies enhance detection performance, and real-world tests confirm the framework's effectiveness. This work advances secure, private and efficient vehicle platooning, improving the reliability of cooperative driving automation. Future work is focusing on federated learning to enhance security of cooperative driving under adversarial attacks.

**NCHRP Research Report 1118: Incorporating Resilience into Transportation Networks**, Chandler Duncan, Jeffrey Harris, David Proffitt, Chandra Khare, Vincent Matheney, Justin Peng, Stephen Fleck, Mary Katherine Duncan, Gabrielle Westcott, Sarah Preisler, Frank Broen, Mihir Thakar, Mark Berndt, Jeannie Beckett, Felipe Aros-Vera and Gwyn Kash, 2024.
Publication available at http:/nap.nationalacademies.org/catalog/27919
*From the foreword*: NCHRP Research Report 1118: Incorporating Resilience into Transportation Networks provides a guide for state departments of transportation and other transportation agencies seeking to define and strategically integrate resilience into transportation networks and network planning. Included with the guide are case studies, tools and other materials to support implementation. The guide and its supporting materials will be useful to transportation agency executives and senior planning managers seeking immediately implementable strategies for defining, avoiding and managing the potential risks and vulnerabilities of transportation networks caused by unpredictable events.

*Related Resources*:

> **NCHRP Web-Only Document 391: Resilience in Transportation Networks, Volume 1: Resilience Case Studies**, Chandler Duncan, Jeffrey Harris, David Proffitt, Chandra Khare, Vincent Matheney, Justin Peng, Stephen Fleck, Mary Katherine Duncan, Gabrielle Westcott, Sarah Preisler, Frank Broen, Mihir Thakar, Mark Berndt, Jeannie Beckett, Felipe Aros-Vera and Gwyn Kash, 2024.
> Publication available at https://nap.nationalacademies.org/catalog/27920/
> *From the background and synthesis:* This report's case studies show various experiences highlighting frameworks, tools, methods and data needs. Increasing the resilience of transportation networks affects transportation operations and many other networks and systems. For example, the transportation network is the backbone of supply chains that produce, transport and deliver critical products. Understanding that transportation networks affect and are affected by other networks and systems is essential. Particular challenges appear as a common theme in most of the case studies: (1) the need for a unified and structured framework for the problem of resilience in

transportation networks, (2) the identification of data-enabled methods and metrics, and (3) the need for accurate, time-sensitive data suitable to make decisions. These needs aligned with the traditional approach, which considers frameworks at a strategic level, methods for tactical considerations and data for operational needs.

**NCHRP Web-Only Document 391: Resilience in Transportation Networks, Volume 2: Network Resilience Toolkit and Techniques,** Chandler Duncan, Jeffrey Harris, David Proffitt, Chandra Khare, Vincent Matheney, Justin Peng, Stephen Fleck, Mary Katherine Duncan, Gabrielle Westcott, Sarah Preisler, Frank Broen, Mihir Thakar, Mark Berndt, Jeannie Beckett, Felipe Aros-Vera and Gwyn Kash, 2024.
Publication available at http://nap.nationalacademies.org/catalog/27921
This publication describes the tools for assessing the resilience of physical infrastructure and institutional arrangements for supporting resilience.

**NCHRP Report 1052: Integrating Resilience Concepts and Strategies into Transportation Planning: A Guide**, Maria Pena, Charles Moser, Mara Campbell and Alan O'Connor, 2023.
Publication available at https://nap.nationalacademies.org/catalog/27192/
This guide offers recommendations to transportation agencies to incorporate resilience into the transportation planning process. It reviews case studies from Arizona, Colorado, Florida, Georgia, Maryland, Minnesota and Oregon DOTs in addition to Vermont Transportation Agency, California Bay Area Rapid Transit (BART), Texas Capital Area Metropolitan Organization and the Danish Roads Directorate. Six building blocks and 27 actions are identified. *From the foreword:*

> The research provides agencies of diverse capabilities, resources and resilience vulnerabilities with concepts and methods to incorporate into existing planning processes to create a framework for addressing resilience in the design and delivery of transportation infrastructure, operations and services. This research will be of particular interest to transportation planning professionals but also to agency decision makers and executives seeking to create a robust and resilient transportation network.

**NCHRP Research Report 970: Mainstreaming System Resilience Concepts into Transportation Agencies: A Guide**, Chris Dorney, Michael Flood, Tim Grose, Paula Hammond, Michael Meyer, Rawlings Miller, Ernest Frazier Sr., Jeffrey Western, Yuko Nakanishi, Pierre M. Auza and John Betak, 2021.
Publication available at https://nap.nationalacademies.org/catalog/26125
*From the foreword:*

> This [g]uide is designed to provide transportation officials with a practical, self-assessment tool to gauge their agency's efforts to improve the resilience of the transportation system by mainstreaming resilience concepts into agency decision-making and procedures. The [g]uide can be applied to a broad array of natural and human-caused threats to transportation systems and services. The [g]uide and a toolkit of supplemental materials present the state of the art and the state of the practice that will be of immediate interest to transportation agency leadership and practitioners.

This comprehensive guidance provides a framework described as "a 10-step process that can be used to identify where changes in an organization and collaborative institutional relationships could be made to better mainstream resilience efforts":

- Step 1: Assess current practice.
- Step 2: Organize for success.
- Step 3: Develop an external communications strategy and plan.

- Step 4: Implement early wins.
- Step 5: Understand the hazards and threats.
- Step 6: Understand the impacts.
- Step 7: Determine vulnerability and prioritize responses.
- Step 8: Identify actions to enhance resilience.

  **System Operations**

  - Step 8A: Assess strategies for enhancing emergency response capabilities and agency preparedness.
  - Step 8B: Identify enhancements to operations and maintenance activities.

  **Capital Improvements**

  - Step 8C: Undertake detailed assessments of exposed assets and new projects.
  - Step 8D: Integrate into asset management.
- Step 9: Program and implement resilience measures.
- Step 10: Monitor and manage system performance.

## Related Research

**"8R Resilience Model: A Stakeholder-Centered Approach of Disaster Resilience for Transportation Infrastructure and Network,"** Syed Ahnaf Morshed, Mahmoud Arafat, Seyedmirsajad Mokhtarimousavi, Sifat Shahriar Khan and Kamar Amine, *Transportation Engineering,* Vol. 4, June 2021.
Publication available at
https://doi.org/10.1016/j.treng.2021.100058
*From the abstract*: Infrastructure and network resilience directly or indirectly deal with the impact of risks, criticalities, emergencies and stakeholders. It is evaluated based on the retrieval of system functionality during global setbacks such as natural disasters, man-made disasters, etc. Despite inherent complexities and posed threats, proper scientific methods to evaluate the transportation infrastructure and network resilience from the users' point of view [are] absent. This study developed a unique "8R Resilience Model," which is an information management tool based on resilient concepts for assessing transportation infrastructure and network resilience. The findings of this study present opportunities to influence policymakers to reassess the disaster resilience of the transportation system during a global crisis. The proposed 8R Resilience Model provides a dynamic stakeholder-centered assessment strategy of disaster resilience. A multi-criteria decision analysis (MCDA) process comprising of the 8R Resilience Model, statistical (survey) model, and social media reaction (Twitter) model has been performed for validation. MCDA result suggests that adopting the dynamic 8R Resilience Model combined with operational resilience metrics is more beneficial in terms of assessing the criticality of any transportation infrastructure than using models developed from survey data and social media reactions.

**"Emergence of Resilience as a Framework for State Departments of Transportation (DOTs) in the United States,"** John Renne, Brian Wolshon, Pamela Murray-Tuite and Anurag Pande, *Transportation Research Part D: Transport and Environment*, Vol. 82, May 2020.
Citation at https://www.sciencedirect.com/science/article/abs/pii/S1361920918309519?via%3Dihub
*From the abstract:* State [d]epartments of [t]ransportation (DOTs) in the United States are responsible for a large portfolio of transportation modes and services, including passenger and freight systems. These responsibilities include operations under routine conditions and during incidents and events that result from various natural and human-caused hazards. During unexpected events, disruptions and reductions in service result in requiring the reallocation and reassignment of personnel, modal, and economic resources. To better prevent and respond to the effects of service disruptions, the concept of

resilience has emerged as an important framework, within which, DOTs across the United States are using to plan for the occurrence of threats. In this paper, the key findings of recent reviews of literature and practice related to resilience among state DOTs in the United States are summarized. The review effort focused on a range of risks faced by transportation agencies including climate change, terrorism, cyber-attacks, and aging infrastructure and the ways in which DOTs are confronting them in practice. The topics of this paper range from the fundamental, including definitions of transportation resilience; to the more complex such as examinations of risk, vulnerability and threats; to the most sophisticated topics including administrative-level efforts to conceptualize evolving transportation planning and policies within a resilience framework.

**"Smart Security?: Evaluating Security Resiliency in the U.S. Department of Transportation's Smart City Challenge,"** Kate Beck, *Transportation Research Record 2604*, Issue 1, January 2017.
Citation at https://journals.sagepub.com/doi/10.3141/2604-05
*From the abstract*: Smart city initiatives, which involve the connection and automation of city systems and services through the use of information and communication technology, offer significant opportunities to improve efficiency and address many environmental, economic and social issues faced by U.S. cities. However, as systems become increasingly connected and automated, these systems and the people whom they serve become more vulnerable to an array of security threats, including cybersecurity attacks and attacks on the physical infrastructure and human lives. This paper focuses on how U.S. cities plan to mitigate and respond to the security risks that may arise from the integration of technology into transportation systems and connecting transportation system databases. After examining the U.S. Department of Transportation's recent competition Beyond Traffic: Smart City Challenge, this paper evaluates 32 of the 77 first-round applications to the Smart City Challenge submitted by midsize American cities. The paper provides a set of criteria to evaluate the resiliency of the applicants' transportation systems, that is, the ability of the cities to withstand and respond to security threats and changing conditions. These criteria include the responses of cities to a range of security risks, the response to unknown risks, plans to accommodate risks, and whether cities plan to work with private or public partners to develop security mitigation and response strategies.

# Contacts

CTC engaged with the people below to gather information for this investigation.

## State Agencies

### Georgia

Emily Fish
Director of Emergency Operations
Georgia Department of Transportation
470-602-0255, efish@dot.ga.gov

### Hawaii

Genevieve Hilliard Sullivan
Climate Resilience Manager
Hawaii Department of Transportation
808-587-2216, genevieve.h.sullivan@hawaii.gov

### Michigan

Todd Bechler
Safety and Security Administrator
Michigan Department of Transportation
517-614-8031, bechlert@michigan.gov

### Minnesota

Erin Meier
Planner, Emergency Management
Minnesota Department of Transportation
651-335-0993, erin.meier@state.mn.us

### Pennsylvania

Jonathan Fleming
Chief Executive Director of Highway Administration
Pennsylvania Department of Transportation
717-772-1771, jonfleming@pa.gov

### Rhode Island

Christos Xenophontos
Assistant Director, Planning Division
Rhode Island Department of Transportation
401-563-4400,
christos.xenophontos@dot.ri.gov

### Washington

John Himmel
Emergency and Security Manager
Washington State Department of Transportation
360-705-7973, john.himmel@wsdot.wa.gov

### Wyoming

Ed Fritz
Policy and Planning Analyst III
Wyoming Department of Transportation
307-777-3818, ed.fritz@wyo.gov

## Federal Agencies

Igor Linkov
Senior Manager, Engineer Research and Development Center
U.S. Army Corps of Engineers
617-233-9869, igor.linkov@usace.army.mil

## Private Sector Organizations

Kevin Maggay
Government Relations
International Motors, LLC
858-254-7556, kevin.maggay@navistar.com

Geoff Danker
Public Policy and Planning Manager
Southern California Gas Company
913-940-7389, gdanker@socalgas.com

# Appendix A: Survey Questions

The online survey represented below was distributed via email to the member list of the AASHTO Committee on Transportation System Security and Resilience and selected contacts identified by the project panel.

**Caltrans Survey on Resiliency Strategies for Unplanned Events**

The California Department of Transportation (Caltrans) has identified resiliency goals related to climate action in the Caltrans 2020-2024 Strategic Plan and California Transportation Plan 2050. The latter plan also includes the goal of creating a resilient transportation system.

For Caltrans, resiliency is defined as the ability to respond to and recover quickly from unplanned events. To expand the current focus on resiliency related to climate change, Caltrans is preparing to develop resiliency strategies to address unplanned events, beginning with the following threats to transportation infrastructure:

- Man-made events and physical attacks.
- Cyberattacks and technologies.
- Nuclear blasts.
- Power blackouts or significant power loss.

With the survey below, Caltrans is seeking information from state transportation agencies and other stakeholders with experience developing resiliency strategies in one or more of the categories of unplanned events listed above. (Each unplanned event will be described in more detail as you complete the survey.) We estimate the survey will take 20 minutes to complete. We would appreciate receiving your responses by **Friday, October 25**.

The final report for this project, which will include a summary of the responses received from all survey participants, will be available on the Caltrans website.

If you have questions about completing the survey, please contact Chris Kline at chris.kline@ctcandassociates.com. If you have questions about Caltrans' interest in this issue, please contact Tori Kanzler at tori.kanzler@dot.ca.gov.

Thanks very much for your participation.

(Required) Please provide your contact information.

Name:
Agency:
Title/Division:
Email Address:
Phone Number:

(Required) Has your agency developed resiliency strategies for unplanned events, other than climate change, such as those listed in the survey introduction?

- Yes (Skipped the respondent to **Resiliency Strategies for Selected Unplanned Events**, **Assessment** and **Wrap-Up**.)

- No, but we have interest in preparing resiliency strategies for unplanned events. (Skipped the respondent to **Interest in Developing Resiliency Strategies** and **Wrap-Up**.)
- No, and we have no plans for or interest in developing resiliency strategies for unplanned events. (Skipped the respondent to **Wrap-Up**.)

**Resiliency Strategies for Selected Unplanned Events**

**Introduction**

Where applicable, please share the resiliency strategies your agency has developed for the following categories of unplanned events:

- Man-made events and physical attacks
- Cyberattacks and technologies
- Nuclear blasts
- Power blackouts or significant power loss

For each unplanned event below, examples or impacts of the event are followed by an opportunity to provide information about the resiliency measures your agency has established.

**Man-Made Events and Physical Attacks**

The resiliency strategies Caltrans is seeking are *in response* to unplanned man-made events such as explosions, fires and excavations, or preparations related to strengthening infrastructure, not preparations *to suppress* these events. Examples of these events that impact physical and human assets:

- Targeting agency infrastructure, causing destruction of physical assets and operations
- Targeting agency personnel, resulting in deaths or injuries

1. Has your agency attempted to identify the geographic locations where unplanned man-made events and physical attacks are most likely to occur?
    - Not applicable
    - No
    - Yes (Please describe this assessment.)
2. Has your agency conducted any work in this threat area that involved the collaboration of federal, state and/or local partners?
    - Not applicable
    - No
    - Yes (Please describe this collaboration.)
3. Please describe your agency's resiliency efforts related to unplanned man-made events and physical attacks. (*If your agency has not developed resiliency strategies for this type of unplanned event, please skip to the next event category*.)

    **Preventive measure(s):**
    **Reactive mitigation measure(s):**
    **Additional information:**

**Cyberattacks and Technologies**

Anticipated impacts of cyberattacks:

- Disruption of port operations (maritime, land and air)
- Freight crane disruptions
- Rail line disruptions

- Bridge disruptions
- Charging station disruptions
- Commercial vehicle enforcement facility disruptions
- Delays in project delivery
- Disruption of traffic lights, tollbooths and electronic signs
- Blocked access to important files and data, possibly exposing sensitive information
- Potential for accidents, mass chaos, injuries and loss of life due to disruption of critical infrastructure

Anticipated impacts of technologies such as artificial intelligence (AI):

- Metaverse, a virtual world that resembles the physical world where preemptive reconnaissance on targets can be done virtually without being detected.
- ChatGPT (Chat Generative Pre-Trained Transformer) presents increased data risk.

1. Has your agency attempted to identify the geographic locations where cyberattacks are most likely to occur?
    - Not applicable
    - No
    - Yes (Please describe this assessment.)
2. Has your agency conducted any work in this threat area that involved the collaboration of federal, state and/or local partners?
    - Not applicable
    - No
    - Yes (Please describe this collaboration.)
3. Please describe your agency's resiliency efforts related to cyberattacks and technologies such as AI. (*If your agency has not developed resiliency strategies for this type of unplanned event, please skip to the next event category*.)

    **Preventive measure(s):**
    **Reactive mitigation measure(s):**
    **Additional information:**

**<u>Nuclear Blasts</u>**

Anticipated impacts of these events, which cause immediate and long-term destructive effects:

- Blast, thermal and radiation effects that cause significant destruction to transportation facilities, other critical infrastructure and humans
- Electromagnetic pulse (EMP) that disrupts communications and damages electronic equipment
- Certain underwater nuclear events

1. Has your agency attempted to identify the geographic locations where nuclear blasts are most likely to occur?
    - Not applicable
    - No
    - Yes (Please describe this assessment.)
2. Has your agency conducted any work in this threat area that involved the collaboration of federal, state and/or local partners?
    - Not applicable
    - No
    - Yes (Please describe this collaboration.)

3. Please describe your agency's resiliency efforts related to nuclear blasts. (*If your agency has not developed resiliency strategies for this type of unplanned event, please skip to the next event category*.)

   **Preventive measure(s):**
   **Reactive mitigation measure(s):**
   **Additional information:**

**Power Blackouts or Significant Power Loss**

These unplanned events can be caused by technical failure, electrical grid sabotage or attacks such as high-altitude electromagnetic pulse (HEMP). Anticipated impacts of these events:

- Widespread and prolonged power blackout paralyzing transportation facilities, the State Highway System and its operations
- Severe backups, crashes and fatalities
- Long fuel lines or out-of-service gas stations that make it difficult to obtain gas for generators

1. Has your agency attempted to identify the geographic locations where unplanned power blackout events are most likely to occur?
   - Not applicable
   - No
   - Yes (Please describe this assessment.)
2. Has your agency conducted any work in this threat area that involved the collaboration of federal, state and/or local partners?
   - Not applicable
   - No
   - Yes (Please describe this collaboration.)
3. Please describe your agency's resiliency efforts related to unplanned power blackout events. *(If your agency has not developed resiliency strategies for this type of unplanned event, please skip to the next event category*.)

   **Preventive measure(s):**
   **Reactive mitigation measure(s):**
   **Additional information:**

**Assessment**

1. Please describe the benefits to your agency associated with establishing resiliency strategies for unplanned events.
2. What challenges has your agency encountered when developing these resiliency strategies?
3. What lessons learned or best practices can you offer to other agencies developing resiliency strategies for the unplanned events addressed in this survey?

   Lesson Learned or Best Practice 1:
   Lesson Learned or Best Practice 2:
   Lesson Learned or Best Practice 3:
4. Please provide links to documents associated with your agency's development of the resiliency strategies you've described in this survey. Send any files not available online to chris.kline@ctcandassociates.com.

**Interest in Developing Resiliency Strategies**

1. Please briefly describe your agency's interest in developing one or more resiliency strategies and identify the unplanned events for which you plan to develop these strategies.
2. What is needed for your agency to begin developing these resiliency strategies?
3. When do you anticipate beginning work on the resiliency strategies?

**Wrap-Up**

Please use this space to provide any comments or additional information about your previous responses.