UNIFIED RESPONSE TO NATIONAL TRANSPORTATION DISRUPTIONS

Building Blocks to Success Identified by Federal Agencies

Matt Hardison
Dr. Karen C. Levush
Dr. Tim Saad

Approved for Public Release; Distribution Unlimited. Case 24-3340.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Overview

In 2023 in response to sponsor concerns regarding the resiliency of U.S. transportation capabilities against man-made and natural threats, MITRE initiated a research program to identify and assess root cause problems associated with transportation system vulnerabilities to open opportunities to aid the U.S. government in efforts to improve transportation system resiliency. This report presents the findings of one element of that program, Unified Response to National Transportation Disruptions ("Unified Response").

The Unified Response program's goal was to examine methods, challenges, and opportunities to improve aspects of transportation system resiliency. Executed through a series of interagency workshops as well as detailed interviews with government experts, this analysis documents stakeholder challenges, perceived needs, and possible solutions associated with managing these events.

The next phase of MITRE's resiliency work will capitalize on the Unified Response program's findings to examine the policies, procedures, and tools of federal, state, and local government as well as transportation system owners and operators. This examination will lead to specific actionable recommendations and solutions to identify and mitigate risks before an event and to improve the efficiency and effectiveness of a response when a major transportation disruption occurs.

Unified Response Program Findings in Brief

MITRE's Unified Response program engaged 40+ subject matter experts, representing 18 agencies across eight federal departments, in a series of three workshops to ascertain stakeholders' challenges and needs. The program team also met with government officials one-on-one before and after the workshops to ensure stakeholders' equities were represented in the workshops and to further explore the findings from these events in more depth.

Through the first two Unified Response engagements ("Part 1"), MITRE facilitated the government study team in identifying two major categories of perceived need, referred to hereout as "Opportunity Areas," related to solutions for risks stemming from a national-scale transportation disruption:

- *Interagency Information and Analytics*: Including improved structured data sets and information sources that could enable rapid impact analysis, prioritization, and decision making.
- *Government-Industry Coordination*: Methods to improve coordination and synchronization for incidents that require support from multiple organizations.

For the third and final workshop ("Part 2"), MITRE focused on facilitating the government study team in identifying gaps and potential solutions within the Opportunity Areas. From this, government participants proposed 21 solutions (see **Appendix**) and ranked these subjectively by importance and feasibility. This assessment resulted in a prioritized list of three primary areas meriting further investigation. In descending order of priority, they include:

1. Explore improved transportation system data and information – to support work at all phases of incident management.
2. Develop reporting systems/dashboards – to inform management in planning (emerging risks), incident management (impacts), and recovery and restoration (by supporting decision making on prioritizing actions).
3. Continue to improve coordination and communication – through improved standardized reporting requirements, a shared intelligence platform, and training.

This report details the findings of the Unified Response research program and will serve as the basis for subsequent phases of MITRE's transportation resiliency research whose goal is to help all levels of government document, prioritize, advance, and resolve the types of concerns documented in this report to improve the resiliency and efficiency of the U.S. transportation system.

Disclaimer: The findings in this report are a summary and direct result of workshop participants' opinions and deliberations collected by MITRE at the workshops and one-on-one meetings only. MITRE did not validate or perform post-analysis on the prioritization, feasibility, or importance of any gap or recommendation listed in this report. However, MITRE feels that this report should be utilized as a starting point to perform follow-on analysis and deep dives in partnership with government stakeholders as part of a path forward to address the resilient transportation system concerns identified within.

Program Overview

The MITRE Unified Response to National Transportation Disruptions ("Unified Response") study examined methods, challenges, and opportunities for managing and recovering from major transportation disruptions that require a coordinated federal response.[1] Throughout the entire effort, the MITRE team brought together and facilitated a series of workshops and one-on-one sessions for 41 unique transportation sector subject matter experts (SMEs) representing 18 agencies across eight federal departments (**Error! Reference s ource not found.**).

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)
Federal Emergency Management Agency (FEMA)
Intelligence & Analysis (I&A)
Transportation Security Administration (TSA)
Office of Strategy, Policy & Plans

U.S. Department of Transportation

Federal Railroad Administration (FRA)
Office of Intelligence, Emergency Response & Security
Office of Multimodal Freight Infrastructure & Policy (OST-F)
Bureau of Transportation Statistics (BTS)

Department of Justice

Federal Bureau of Investigation (FBI)
National Joint Terrorism Task Force (NJTTF)

Department of Defense

National Security Agency (NSA)
Office of the Under Secretary of Defense for Policy (OUSD(P))
United States Transportation Command (USTRANSCOM)
Surface Deployment & Distribution Command (SDDC)

Department of Commerce

International Trade Administration (ITA)

Department of Energy

Cybersecurity, Energy Security & Emergency Response (CESER)

Office of the Director of National Intelligence

Cyber Threat Intelligence Integration Center (CTIIC)

Department of Interior

Office of the Secretary / NJTTF

Part 1 of the program's research included an exploratory workshop to enhance collective understanding of the challenges associated with a federal unified response to a multi-state or national transportation disruption. The workshop led to the identification of several challenges ("Opportunity Areas"). These were then ranked by government SMEs to determine prioritization and for further exploration in Part 2 of the study.[2] The top Opportunity Areas identified in Part 1 were:

- Interagency Information and Analytics
- Government-Industry Coordination[3]

The Part 2 Solutions Workshop drew on a group of 20 SMEs and stakeholders. Participants collaboratively considered the Opportunity Areas, documented and prioritized them, and recommended potential solutions for further study (see **Appendix** for a complete listing of gaps and recommendations).

This report summarizes the findings from Part 2 of the MITRE Unified Response research program based on the Opportunity Areas identified by the government study team in Part 1. The proposed solutions are ranked in priority in consideration of importance and feasibility as scored by the government workshop attendees and presented in this report as potential next steps to improve a future unified response to a national transportation disruption.

Mapping to the National Response Architecture

The Part 2 Solutions Workshop exercises were framed in the context of the existing National Response Architecture, leveraging the National Response Framework (NRF)[4] and National Incident Management System

[1] This study considered federal procedures, processes, and requirements. A later phase may also integrate other government and owner/operator considerations and requirements.

[2] For a more complete discussion of process and findings for this phase of the work program, see *Exploratory Workshop Findings – Unified Response to National Transportation Disruptions*; April 2024, The MITRE Corporation.

[3] Opportunity Area names were updated from the names used in an earlier phase ("Information and Resource Visibility/Availability" and "Authorities and Procedures") for consistency.

[4] *National Response Framework*, Department of Homeland Security, Federal Emergency Management Agency, https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response, accessed July 10, 2024.

(NIMS)[5] to guide discussions and the identification of specific solutions. This approach ensured that proposed solutions were also grounded in current operational realities and regulatory and procedural frameworks that govern national response to major transportation disruptions.

An integral part of this approach was the introduction of the National Response Framework Incident Response Process (Figure 1) and the three components of NIMS (Figure 2). By considering solutions in the context of the NRF and NIMS, participants were able to draw on established best practices and protocols to foster a discussion focused on the development of clear, practical solutions.

Figure 1: National Response Framework Incident Response Process

Figure 2: Components of National Incident Management System

Methodology

Workshop participants, building on the context of the National Response Architecture, focused on defining specific, cross-organizational challenges or gaps from the Part 1 Opportunity Areas below:

- *Interagency Information and Analytics*, including structured data sets and information resources that could facilitate rapid impact analysis, prioritization, and decision making; and
- *Government-Industry Coordination*, such as solutions to address challenges regarding execution of command and coordination for incidents that cut across multiple organizations.

Twenty-one solutions were identified across the Part 1 Opportunity Areas. The majority were associated with the NRF's Pre-Incident phase, though participants also noted that many solutions that supported the Pre-Incident phase could also support the Response and Recovery & Restoration phases.

Participants rated proposed solutions across two dimensions on a scale of 0 (least) to 10 (most) to arrive at an overall prioritization:

- Importance, accounting for organizational/leadership priorities, the potential to enhance a unified response, and broader national interests; and
- Feasibility, which considered factors such as the level of difficulty, cost, time commitment, and the necessary level of leadership or organizational support required to implement each solution set.

The solutions and relative rankings (from least to most)[6] are shown on the following page (Figure 4).

[5] *National Incident Management System*, Department of Homeland Security, Federal Emergency Management Agency, https://www.fema.gov/emergency-managers/nims, accessed July 10, 2024.

[6] Four (of the 21) solutions across the two Opportunity Areas were not prioritized (N/P) during the exercise due to time constraints. See the appendix for a complete list of the gaps and corresponding solutions.

Figure 4: Proposed Solution Sets and Prioritization

Interagency Information & Analytics

A. Operations Data
1. Centralized repository for incident information
2. Shared event status & statistics reporting platform
3. Pre-incident training & tabletops/networking sessions

B. Threat Intelligence Analysis & Communications
1. Shared threat intelligence platform
2. Interagency analytic/intelligence sharing partnerships

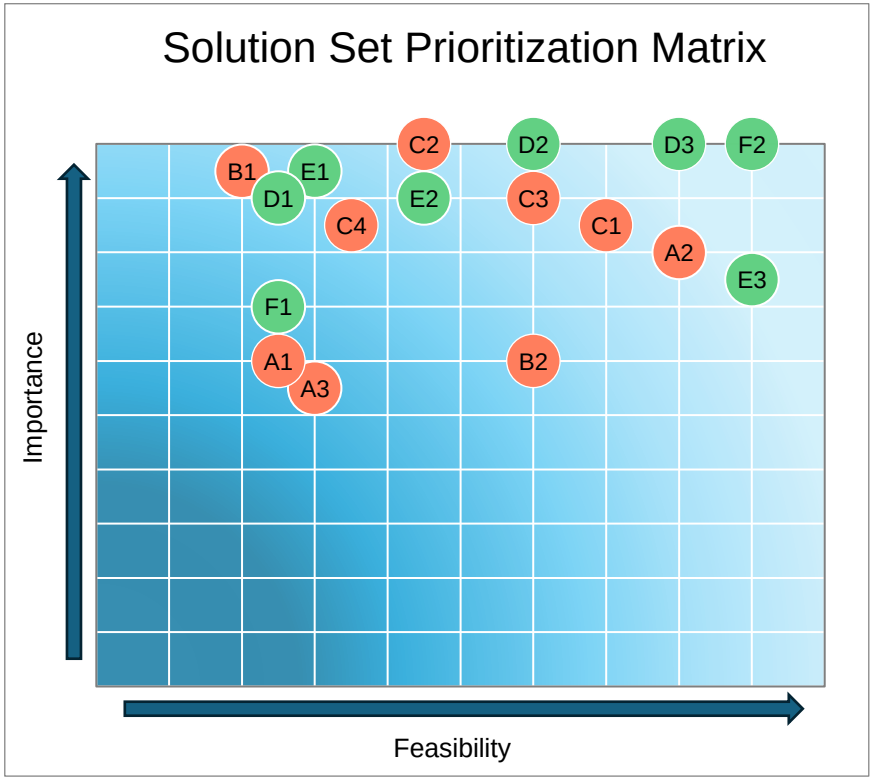
C. Analysis of Risks, Impacts
1. Models/tools to project impacts
2. Best practices clearinghouse
3. Real-time asset condition & visualization tools
4. Real-time commodity flows

Government-Industry Coordination

D. Unified Federal System for Cyber Incident Reporting
1. Finalize CIRCIA rulemaking
2. Connected mode communication networks
3. Standardize incident reporting requirements

E. Incident Communication
1. Publicize specific incident procedures
2. Conduit for queries
3. Federal resources allocation & access information

F. Processes
1. National Response Framework training
2. Evaluation criteria for recovery actions



Prioritization Matrix of Proposed Solution Sets Based on Importance and Feasibility

Findings

This program, in partnership with agency participants, identified specific opportunities to enhance the effectiveness and efficiency of federal government coordination in each of the three phases of the NRF incident response process.

As context for these solutions, participants highlighted challenges that may affect feasibility such as:

- Interagency Requirement: Many proposed solutions will deliver benefits for more than one agency. In these cases, it may be challenging to determine a lead agency to invest in and lead the development of a solution.
- Solution Connectivity: Solutions were not exclusive to a given topic area or mode of transportation. Many proposed solutions also align with and, to some degree, complement others. This suggests that a long-term plan to address challenges and implement solutions must be designed strategically to accommodate intermodal connections and build incrementally toward a broader solution.
- Resources: Funding, staff resources, and time were frequently mentioned as constraining factors in addressing challenges associated with each of the three stages of incident management (Pre-incident, Response, and Recovery & Restoration). Finding practical solutions therefore also means ensuring that they can operate without incremental operating costs or be supported financially and organizationally.
- Technical Feasibility: The feasibility of solutions focusing on data collection depends on scale, timing, and agency authority:
  - Large-scale, integrated, intermodal data collection will require phased implementation.
  - Federal agency authority to acquire data varies by mode. Where limitations exist, options may entail either (a) agreeing to confidentially sourced (non-attributable) data, or (b) securing data from the owner/operator directly only at the time of an incident—meaning no pre-planning is possible.

Next Steps

In consideration of the findings above and follow-on discussions with workshop attendees, prioritized next steps to mitigate the gaps found by the study team include those listed below (detailed in **Appendix**). MITRE has begun discussions with relevant federal sponsors and internal experts to evaluate the feasibility of each of the program concepts and determine appropriate next steps.

- **Explore Improved Transportation System Data and Information.** Government, industry, and other stakeholders require improved access to data that directly informs decision making. Such data could provide insights to help anticipate, manage, and recover from incidents at all levels of government. Data and information development work must also include tools to access and report. This includes (a) detailed modal performance data; (b) modeling to support planning, response, and recovery; and (c) systems to ingest, share, and report incident data (Aligned Recommendations A1, A2, C1, C3, C4).
- **Develop Dashboard Reporting.** Beyond building transportation data sets, agencies need a corresponding reporting or dashboard system to ensure data and information are readily accessible in a format that supports rapid and effective decision making. Participants recommended that such a program capitalize on the ongoing interagency Tabletop Exercises (TTXs) to test and evaluate potential reporting and dashboard systems (Aligned Recommendations A2, B1, B2).
- **Continue to Improve Government Coordination.** Recent policies and programs, such as National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22[7]), have advanced and improved coordination. Participants recommended continued regulatory and process improvements. This included finalizing the Cyber Incident Reporting for Critical Infrastructure Act rulemaking (Recommendation D1), as well as actions to improve incident and interagency coordination, such as a shared intelligence platform, standardized reporting requirements, better training, and increased engagement through participation in TTXs (Aligned Recommendations A2, A3, B1, D3, E2, F1).

[7] See *National Security Memorandum on Critical Infrastructure Security and Resilience*, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/, April 30, 2024.

Appendix
Gaps and Recommended Solutions by Major Opportunity Area

	Gap	Recommendation
	Interagency Information and Analytics *Operations Data, Threat Intelligence Communications, and Supporting Analytics*	
	A. Operations Data	
1	Absence of a centralized repository for sharing of all incident-related information, analysis, and data.	***Centralized repository for incident information.*** Implement a user-friendly, centralized repository for uploading and consolidating incident-related information, similar to FEMA's National Business Emergency Operations Center Dashboard,[8] to facilitate sharing of incident-related information among federal agencies.
2	Lack of a primary federal common operating system (e.g., Homeland Security Information Network, Web-based Emergency Operations Center) that provides a unified picture during events, especially those affecting supply chains or infrastructure.	***Shared event status and statistics reporting platform.*** Examine the feasibility of a shared event status and statistics reporting platform for use during events and capitalize on TTX program(s) to: (a) test the availability and use of these systems and (b) ensure that all agencies' goals are coordinated and integrated through the system solution.
3	Unclear roles and responsibilities, particularly when knowledge is not shared among colleagues or preserved with personnel change; especially if not codified into policy.	***Pre-incident training and tabletops/networking sessions.*** Undertake pre-incident training and tabletops/networking sessions to: (a) network and establish relationships across agencies, (b) practice with clear examples, and (c) share lessons learned with colleagues following such sessions.
	B. Threat Intelligence Analysis & Communications	
1	Lack of clarity on what programs cybersecurity services entities are enrolled in across the federal government and what data they collect.	***Shared threat intelligence platform.*** Develop a central database fed by all federal partners that delivers the various services an entity may be enrolled in combined with a shared threat intelligence platform that allows users to query against collected data.
2	Lack of established information/intelligence sharing partnerships between USDOT, CISA, and the intelligence community.	***Interagency analytic/intelligence sharing partnerships.*** Establish formal Memorandums of Understanding or analytic/intelligence sharing partnerships between USDOT, intelligence agencies, and DHS CISA to regularly share early warning and mitigations to known cyber threats.
N/P[9]	The ability to quickly and accurately determine whether a physical impact, such as a malfunction or operational disruption, is the result of a malicious act or an accident. This has implications for understanding if it is an isolated incident or the first in a potential series of incidents.	Capitalize on mandatory/required reports of incidents with unknown cause across modes for analysis of trends over time to identify patterns of specific incident features or circumstances that warrant investigation of possible cyber activity.
N/P[9]	Entities sharing intelligence about potential cyber threats often rely on goodwill—sharing can be disrupted when personnel change.	Develop standard operating procedures that include established position-based lines of communication for sharing information about potential cyber threats across agencies.

[8] https://www.fema.gov/business-industry/national-business-emergency-operations-center

[9] Four (of the 21) solutions across the two Opportunity Areas were not prioritized (N/P) during the exercise due to time constraints.

	Gap	Recommendation
	Interagency Information and Analytics ***Operations Data, Threat intelligence Communications, and Supporting Analytics***	
	*C. **Analysis of Risks, Impacts***	
1	Lack of understanding of how disruptions or delays differentially impact various industries in the United States. For instance, certain industries that rely heavily on bulk commodities might be more affected than those that can easily divert their shipments via truck.	***Models/tools to project impacts.*** Conduct in-depth analyses or studies that look beyond immediate impacts and explore how disruptions affect different industries. This could involve developing models or tools that can predict the impacts of disruptions on various sectors, considering their specific characteristics and dependencies.
2	Lack of consistency in availability of and access to data and tools for decision making to perform vulnerability assessments and to implement resiliency measures.	***Best practices clearinghouse.*** Create a program focused on the current state of practice, identifying data and tools already being used and making them accessible to all stakeholders. This would involve coordinating efforts across modal offices and consolidating under one umbrella for uniform access. The program would cover all hazards and all modes of transportation, including nonconventional modes like pipelines.
3	Lack of a central source of data on operations to help answer questions related to the expected duration of delays, path to normalcy, and effects on the movement of goods.	***Real-time asset condition & visualization tools.*** Develop real-time asset management condition and visualization tools to see how impacts are unfolding on a timely basis.
4	At least one-month delay in data currently available for analyzing the impact of incidents on the shipment of goods throughout the U.S.	***Real-time commodity flows.*** Evaluate the feasibility of a real-time dashboard that tracks movement of shipments and particular commodity flows.
	Government-Industry Coordination *Systems and Processes*	
	D. Unified Federal System for Cyber Incident Reporting	
1	Incomplete implementation of Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA; notice of proposed rulemaking is out but has not been finalized[10]).	***Finalize CIRCIA rulemaking.*** Finalize CIRCIA rulemaking to define reporting requirements for critical infrastructure entities and responsibilities for federal agencies.
2	Lack of a network that enables all key players to quickly connect and effectively communicate in real time once a cyber incident is identified, especially when different industries may be interconnected and affected by the same incident.	***Connected mode communication networks.*** Establish communication networks that reflect the interconnectedness of different industries. A unified system for current federal reporting requirements can be leveraged so that an incident report by one entity in one industry can trigger communication to other entities across other industries likely to be affected by the same incident.
3	Wide variation in current federal cyber incident reporting regulations with respect to (a) what constitutes a reportable incident, (b) the process for reporting an incident, (c) which entity receives the report, (d) what information must be reported, and (e) how long an entity has to report the incident.	***Standardize incident reporting requirements.*** Standardize and clarify federal cyber incident reporting regulations, including with an integrated platform for reporting cyber incidents to allow for immediate sharing of relevant information from an incident report to appropriate federal entities. This enables elimination of duplicative reporting requirements across the cyber incident reporting landscape and provides a potential pathway for eventual harmonization of federal cyber reporting requirements.

[10] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

	Gap	Recommendation
	Government-Industry Coordination *Systems and Processes*	
	E. Incident Communication	
1	Lack of established or confirmed interagency information request procedures, especially when the National Response Coordination Center is not activated. For example, an agency may submit a request for a consequence analysis, and then a request for the same analysis may come in from another federal entity. Lack of clarity as to whether requests are entirely separate asks with different needs can lead to duplication or confusion due to the same question being asked multiple times from the same source.	***Publicize specific incident procedures.*** Develop and publicize procedures during steady state for adoption throughout all phases of incident response. This procedure would make readily evident how requests should be routed and received through the event's designated relevant resource, such as an SRMA, DHS, or DOD, allowing for effective triage and timely response and avoiding duplicative efforts.
2	Multiple agencies requesting information from owner-operators, which may hamper their actions due to the volume of requests (e.g., a private entity that is getting inundated by potential regulators, potential media, and others).	***Conduit for queries.*** Standardize and establish a specific conduit to direct questions to and from the appropriate organizations, particularly owner-operators within critical infrastructure during incidents.
3	Lack of clarity on the source of funding and expertise for remediation within the federal government and the criteria for critical infrastructure entities to access these resources.	***Federal resources allocation & access information.*** Establish or clarify federal authorities with explicit guidance from federal leadership on how to allocate and access remediation resources, including allocation of federal funding or expertise.
	F. Processes	
1	Not all agencies fully understand the NRF, particularly in the context of a national-scale incident, such as one that could cripple the transportation sector and the economy.	***National Response Framework training.*** Enhance understanding of the NRF, possibly through comprehensive briefings, training, or documentation.
2	Prioritization of needs during the Recovery and Restoration phase after an incident. There can be a disconnect between what people perceive as urgent needs (e.g., personal items stuck in transit) and what is critical for the reconstitution of life and property (e.g., essential supplies).	***Evaluation criteria for recovery actions.*** Develop clear criteria and process/protocol for conducting a systematic and thoughtful evaluation of needs during the initial reconstitution phase. This could involve a phased process where the most critical needs, from the perspective of saving lives and property, are addressed first. Additionally, there could be a role for commercial markets to step in and fill certain gaps, such as providing necessary resources or services.
N/P[11]	Unclear transition of leadership during recovery, specifically who is in charge: Industry / Local / State / Federal / White House.	Establish a clear protocol that delineates the transition of recovery responsibilities from the federal government back to the initial managing entity (industry, local, state, or specific department) after a certain point in the recovery process.
N/P[11]	Lack of understanding about the role of Emergency Support Function (ESF) #14 (Cross Sector Business and Infrastructure) in managing lifeline sectors and determining the resources needed to stabilize the Community Lifelines during an incident.	Enhance understanding about the role and utility of ESF #14, possibly through comprehensive briefings, training, or documentation.

[11] Four (of the 21) solutions across the two Opportunity Areas were not prioritized (N/P) during the exercise due to time constraints.