MITRE

MARCH 20 EXPLORATORY WORKSHOP PRELIMINARY FINDINGS

UNIFIED RESPONSE TO TRANSPORTATION DISRUPTION

APRIL 2024

Table of Contents

Executive Summary

With its federal sponsors' support, MITRE is leading a study to examine methods, challenges, and opportunities for managing and recovering from major transportation disruptions that require a coordinated, whole-of-nation response.

Phase 1 of this study, built on in-depth interviews of experts in government and industry, as well as a 7-agency workshop, is designed to advance the collective understanding of risks stemming from a national scale disruption and the requirements for a rapid, unified response to minimize operational, economic, and security risks.

This document presents preliminary findings of Phase 1 and seeks feedback on those findings and recommendations from participants and other stakeholders.

Findings in Brief

Government and infrastructure owner/operators facing a major transportation system disruption must take rapid, effective, and decisive actions to minimize risks. Phase 1 interviews and the associated interagency workshop ("convening") identified three primary themes for challenges in doing so:

- Clarifying Roles, Responsibilities, and Authorities – how do government agencies and industry organize and convene most efficiently and productively?
- Building Data-Informed Decision-Making – what kind of data and information are needed to support decision-making and how is it managed?
- Resolving Barriers to Effective Communications and Collaboration – how can government and industry coordinate and communicate most effectively internally and with the public?

The solutions that were proposed and discussed in each of these categories are presented below.

Clarifying Roles, Responsibilities, and Authorities

- Develop Unified Response Playbook to create common understanding of Unified Coordination Group (UCG) policies and procedures.
- Map authorities and procedures of federal programs and directives to mitigate confusion across policies/directive.

Building Data-Informed Decision Support

- Create information architecture to inform updates and document lessons learned from real-life and simulation events to track trends over time.
- Develop standardized process for assessing risk and escalation in response to transportation disruptions.
- Conduct third-party evaluations of critical response to real-life events to inform updates of standard operating procedures.
- Partner among agencies drawing on existing tools, such as the U.S. Department of Transportation's Freight Logistics Optimization Works (FLOW) and U.S. Customs & Border Protection (CBP) to develop a commodity prioritization modeling and decision framework, integrating commercial solutions, as appropriate.

Resolving Barriers to Effective Communication & Collaboration

- Host regular "red team" conference of government/industry emergency response coordinators and leaders.
- Study challenges of information classification and its impacts on sharing (e.g., over classification, industry clearance) and advance solutions, such as developing a new framework to guide future handling.
- Study the need for a standing interagency task force to respond to transportation disruptions rapidly and efficiently.

Next Steps

The research team will be seeking feedback to further validate the findings of this preliminary report through both direct feedback as well as a follow-on meeting of both the convening's participants and other agency and department staff with expertise and interest in advancing solutions to this challenge space. This report of preliminary findings will then be updated and serve as the basis for a Phase 2 multi-agency convening to advance solutions and actions for senior executive consideration.

Stakeholders who wish to offer feedback, suggestions and ideas for improvement can contact the team directly at resilienttransport@mitre.org.

Introduction/Background

Recent transportation disruptions, such as the 2023 Philadelphia I-95 and Los Angeles I-10 bridge fires as well as the 2024 Key Bridge collapse in Baltimore, have demonstrated the risks that a significant disruption to transportation infrastructure can result in economic repercussions on a broad scale. In 2023, MITRE initiated a self-funded research program examining transportation and logistics resiliency and, more specifically, the federal response to a significant disruption.

Managing and recovering from these events requires a coordinated, whole-of-nation response. Today's process for doing so is set out in the National Response Framework (NRF)[1] and related policy and procedural frameworks.[2] Central to the NRF's incident response, management, and recovery goals is the Unified Coordination Group (UCG). The UCG oversees and coordinates activities of government and private sector response.

MITRE's research goal is to ensure the NRF process works as envisioned, and that the associated federal activities are as efficient and effective as possible. To consider this topic, the research team organized a series of meetings with experts from lead federal agencies and departments to document the understanding of the process, challenges to its implementation, and opportunities to improve upon it.

This document presents the findings from the first phase of that work, specifically including extensive interviews with federal emergency management and response leaders, building to a convening of those leaders to jointly identify pain points and challenges to operationalizing a national response and identify initial improvement opportunities.

Later phases of this work will reengage these leaders, and other relevant stakeholders, to explore, refine and advance possible solutions and methods to improve response effectiveness.

Unified Response Analytic Process

A unified response requires comprehensive plans and common ground governance to establish clear lines of communication, responsibilities, and authority. The analytic process for this research effort leverages a scenario-based approach designed to lead to recommended strategies for strengthening the existing framework for a unified response across the federal government.

- ***Phase 1*** of this work was designed to advance the collective understanding of risks to the U.S. transportation system from a national scale disruption and the importance of a rapid, unified response to minimize operational, economic, and security risks.
- ***Phase 2*** will seek to identify and recommend specific solutions and define multi-agency and government/industry approaches for advancing improvements based on Phase 1 outcomes.

[1] See National Response Framework, Department of Homeland Security, 4th Edition, October 28, 2019, https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response.

[2] See also, for example, *National Disaster Recovery Framework*, *National Cyber Incidence Response Plan*, and Presidential Policy Directives (PPDs): Critical Infrastructure Security and Resilience (PPD-21), U.S. Cyber Incident Coordination (PPD-41), and Enhancing Domestic Incident management (PPD-44).

Phase 1 Approach

Phase 1 included two steps—one-on-one or small group interviews with experts from lead federal agencies and departments, followed by a multi-agency convening with the same experts as well as additional agency staff identified through the interview process. The interviews identified initial themes and topics that were later used in organizing the exercises and guiding the conversation of the broader convening.

Pre-Convening Interviews

MITRE conducted dozens of interviews in advance of convening experts from lead federal agencies and departments. The purpose of these interviews was to familiarize interviewees with the process, introduce the scenario that would be leveraged throughout Phase 1 as a foundation for discussion, and seek their initial reactions and recommendations—both to the disruption scenario itself and on the current state of federal incident response policies and processes. Interviewees were also invited to participate in a multi-agency, exploratory workshop ("convening").

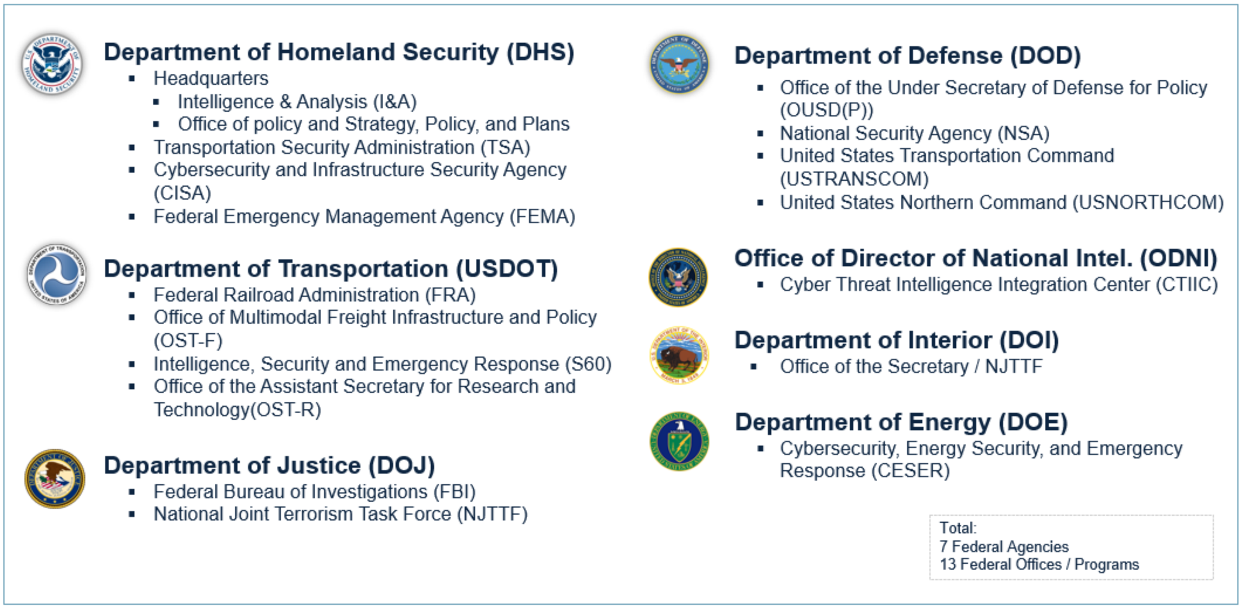
Interview findings were used to improve the scenario parameters and to guide the planned convening discussion by establishing common themes from across multiple participants and agencies. Initial themes included:

- **Establish framework and leadership structure** specific to the disruptions to effectively respond to incidents, and cyber incidents, specifically.
- **Ensure a swift and secure recovery process after a disruption by incorporating insights into the economic impacts** of the disruption to the operating elements affected and ensuring the threat has been fully neutralized.
- **Build a consistent severity threat assessment method across agencies** – to address challenges from different risk evaluations and associated resource commitments.
- **Ensure federal agency authorities align with responsibilities** in collaborating across agencies, such as with TSA, CISA, transportation and intelligence agencies.
- **Seek "One Voice"** from each agency represented in a UCG to ensure consistent messaging for interagency coordination.

Convening

In March 2024, 26 experts from 7 different federal agencies came together to jointly explore the challenges in organizing and coordinating a unified federal response as well as possible solutions. Figure 1 provides a listing of participating agencies, offices, and programs. Additional participants were invited, though unable to participate. The research team hopes to include additional entities from across government and industry in future convenings.

The meeting design focused on setting the stage for participants to tackle a complex problem that requires a whole-of-nation response. The convening integrated proven methods to foster open communication, enhance cross-agency networking, and build a shared commitment to tackle long-running challenges.



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

Department of Transportation (USDOT)
- Federal Railroad Administration (FRA)
- Office of Multimodal Freight Infrastructure and Policy (OST-F)
- Intelligence, Security and Emergency Response (S60)
- Office of the Assistant Secretary for Research and Technology(OST-R)

Department of Justice (DOJ)
- Federal Bureau of Investigations (FBI)
- National Joint Terrorism Task Force (NJTTF)

Department of Defense (DOD)
- Office of the Under Secretary of Defense for Policy (OUSD(P))
- National Security Agency (NSA)
- United States Transportation Command (USTRANSCOM)
- United States Northern Command (USNORTHCOM)

Office of Director of National Intel. (ODNI)
- Cyber Threat Intelligence Integration Center (CTIIC)

Department of Interior (DOI)
- Office of the Secretary / NJTTF

Department of Energy (DOE)
- Cybersecurity, Energy Security, and Emergency Response (CESER)

Total:
7 Federal Agencies
13 Federal Offices / Programs

Figure 1 Participating Federal Agencies - March 2024 Convening

The convening was organized around four exercises (Figure 2) designed to jointly explore processes, pain points, and challenges associated with the federal response to a national transportation disruption viewed through the lens of a targeted disruption scenario (Appendix A). The disruption presented was the result of a concerted cyber campaign—beginning with cyber-attacks on two key components of rail infrastructure, followed by a cyber-attack on a pipeline. Information about each additional disruption event was provided throughout the day, including the ripple effects from supply chain disruptions. |

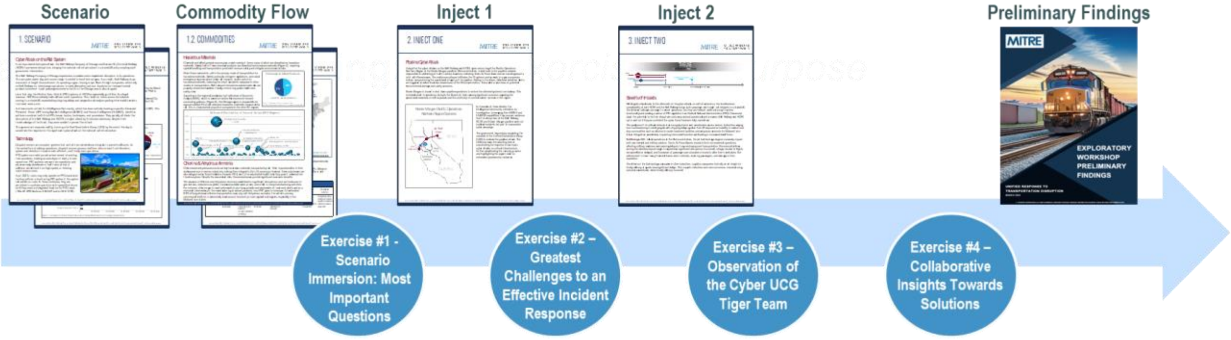

Scenario
1. SCENARIO
Commodity Flow
1.2 COMMODITIES
Inject 1
2. INJECT ONE
Inject 2
3. INJECT TWO
Preliminary Findings
MITRE
EXPLORATORY WORKSHOP PRELIMINARY FINDINGS
Exercise #1 - Scenario Immersion: Most Important Questions
Exercise #2 – Greatest Challenges to an Effective Incident Response
Exercise #3 – Observation of the Cyber UCG Tiger Team
Exercise #4 – Collaborative Insights Towards Solutions

Figure 2 Convening Exercises

A set of high-level themes, along with more detailed pain points, emerged from attendee discussion over the course of each exercise. In the latter half of the convening, participants began to identify an initial set of solution opportunities for more rigorous exploration.

Periodically during the convening, the team revisited participant expectations, engagement, and key takeaways to advance findings.

Summary Findings

Hundreds of participant-provided inputs and detailed notes captured throughout the session were analyzed to extract and summarize key findings and opportunities. The following sections provide a breakdown of data and findings identified throughout the convening.

Exercise 1 – Scenario Immersion: Most Important Questions

For Exercise 1, attendees were asked to consider the cyber-attack disruption scenario and commodity flow information and identify the most important questions critical for a UCG to consider when coordinating an efficient and effective response. The questions were then categorized to elicit key themes for exploration (Figure 3, Table 1). Next, attendees voted to indicate which two of the key themes they viewed as the most important to mounting an effective response. Figure 3 provides a visual representation of the votes assigned across the key themes of questions that emerged from the 'Most Important Questions' exercise.

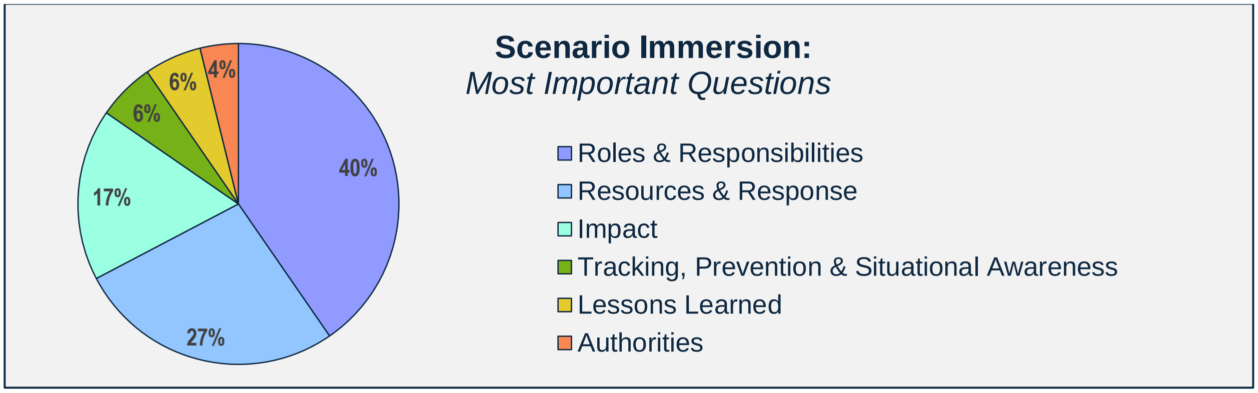


Figure 3 Scenario Immersion: Most Important Questions Exercise

Question Themes	Sample Questions
Roles & Responsibilities (40%)	*Who is designated as the lead?* *What are the responsibilities of government agencies to assist in the response?*
Resources & Response (27%)	*How can we get trains running without comprised systems?* *What are the needs of the affected railroads?* *What long-term options are there?*
Impact (17%)	*Is there a risk to public safety?* *When do the railroads expect to be operational?*
Tracking, Prevention & Situational Awareness (6%)	*What are the vulnerabilities of the system?* *Have we seen similar activity before?* *What logs do we have for attribution/investigation?*
Lessons Learned (6%)	*How can the government respond better in the future to prevent this from happening again?*
Authorities (4%)	*What additional authorities are required for successfully addressing this scenario (e.g., PTC, hours of service, manning)?*

Table 1 Sample Critical Questions Within Each Category

The following descriptions provide insights into the contents of the top three key themes, encompassing the most important questions participants viewed as critical for a UCG to consider when coordinating an efficient and effective response:

- ‘Roles & Responsibilities’ (40%) comprised of questions related to the formation of the UCG and its leadership, such as what circumstances trigger the formation of a UCG, who is designated to lead, and what are the responsibilities of UCG members and their respective agencies.
- ‘Resources & Response’ (27%) comprised of questions focusing on the process of developing a response strategy, including defining the specific lines of effort and associated activities, as well as determining whether the affected railroad company and designated leads of response activities would have the necessary resources.
- ‘Impact’ (17%) comprised of questions related to operational impacts, movement of goods, overall safety to the population, time of impact, and value of impact—ideally with insights into commodities and sectors.

Exercise 2 – Risks to Successful Execution

In Exercise 2, attendees were asked to identify actions that would ensure failure of a federal response. From this list, attendees individually voted on the actions they believe already regularly occur in response to national disruption events and which ideally should be rectified in the near term.

This analysis considered only the actions that received votes. These were grouped into underlying themes (Figure 4) and the following descriptions provide insights into the contents of the five categories that received the greatest number of votes.

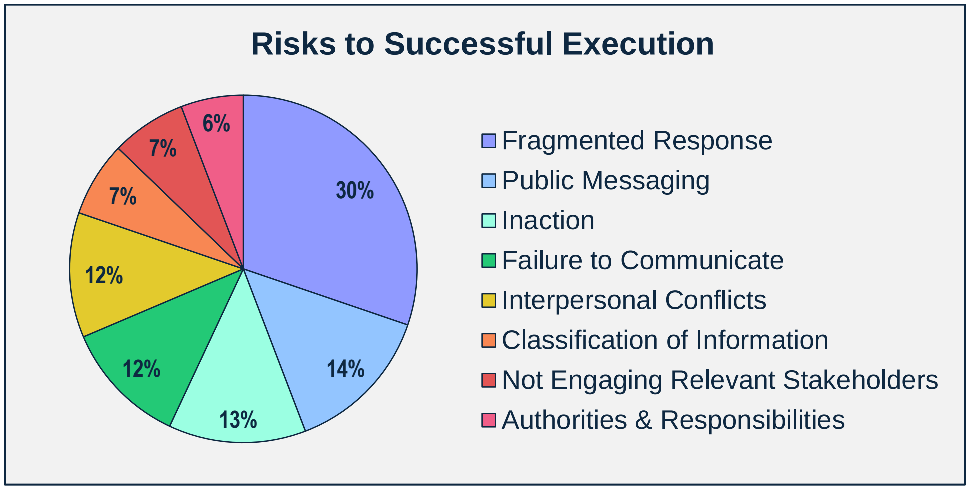


Figure 4 Risks to Successful Execution Exercise

Content in the largest category of “Fragmented Response” (at 30%) comprised of responses that indicated a lack of collaboration and unity in the response strategy, including a siloed response by each agency (resulting in conflicting information and lack of direction) or failure to engage with SME’s and Sector Risk Management Agencies (SRMAs).

The second largest category of “Public Messaging” (at 14%), encompassed acts of information dissemination that would undermine the federal incident response process, such as poor messaging or premature press releases. “Inaction” was the third largest category (at 13%) and comprised challenges associated with taking the necessary and appropriate actions and decisions, including assuming someone else will handle the situation, or being unwilling to act or make a decision when a quick decision is required.

Both categories of “Interpersonal Conflicts,” such as assigning blame or personality conflicts, as well as “Failure to Communicate” received equal number of votes (at 12%). It is of note that “Failure to Communicate” is distinct from “Public Messaging” in that its emphasis is on communication breakdowns or an outright lack of or absence of communication internally within an organization, as opposed to uncoordinated or poor communication strategies used by an organization to reach the public.

Exercise 3 – Observation of the Cyber UCG Tiger Team

For Exercise 3, eight attendees, one representing each participating agency's perspective, role-played a UCG formed in response to the use case scenario. The remaining convening attendees observed their discussion and later contributed to the review.

Figure 5 Cyber UCG Tiger Team

The Tiger Team (Figure 5) was composed of representatives from, DHS-TSA, DHS-CISA, DOE, DOJ-FBI, DOD, ODNI, USDOT-FRA, and DOI. The Tiger Team discussion centered on the roles and perspectives of each agency represented in the group. This process revealed different viewpoints in several key areas, including: (1) which agency adopts the lead role, (2) what are the critical lines of effort and associated activities, and (3) which agency/role leads public messaging. Some discussion also centered on the responsibility of specific agencies to share critical information or intelligence with other federal agencies.

Concerns also arose over differences in how agencies assess the level of severity and impact of the incidents. For example, one agency stated that, from their perspective, the severity of the threat posed by the incidents did not rise to a "significant" level disruption where agency intervention would be necessary, despite the foreseeable cascading impacts of the incidents on their respective sector.

The group's discussion suggested that individuals representing their respective agencies may underestimate how their actions (or inactions) can affect the overall operational scenario and may overlook instances where interests overlap or align with other agencies.

Exercise 4 – Collaborative Insights

Exercise 4 was designed to facilitate open dialogue and foster collaborative problem-solving among the convening attendees. The exercise was the culmination of the convening's insights, discussions, and ideas generated throughout the day, with the primary goal of developing potential solutions to identified challenges.

The exercise followed a structured approach, where attendees engaged in small group discussions while responding to a set of pre-defined questions. These questions were based on the key issues and challenges that had been identified throughout the pre-convening interviews, as well as in the previous exercises during the convening. Each question was designed to elicit meaningful discussion that would lead to collaborative identification of innovative solutions.

Patterns emerged across responses that were then organized into broader "solution set" categories. The subsequent figures visually depict the "solution set" categories that surfaced from the discussions around five distinct questions during the exercise. Accompanying each figure is a table that consolidates the responses categorized under each solution set and begins with the category that received the greatest number of votes (indicating agreement with other attendees written responses).

Q1. Enhance Processes for Implementing Lessons Learned

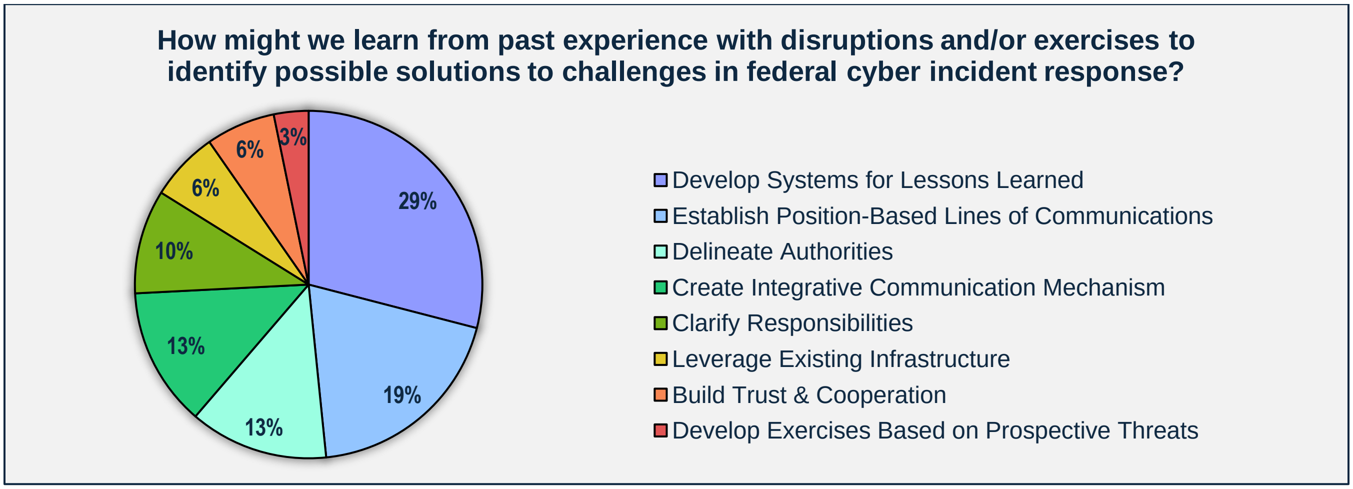


Figure 6 Enhance Processes for Implementing Lessons Learned Solution Set Themes

SOLUTION SET” CATEGORY	SAMPLE RESPONSES
Develop Systems for Lessons Learned	• Maintain a central repository of learning from exercises across agencies • Create a system to share information and enable successive generations in specific roles to look at and learn from the information from prior incidents & exercises • Establish ‘lessons learned’ offices across agencies to archive, share, and make lessons accessible to others
Establish Position-Based Lines of Communications	• Address challenge of maintaining necessary agency contacts due to personnel turnover • Create a communications matrix identifying positions for contacts, as opposed to identifying personnel
Delineate Authorities	• Clarify authorities to enforce improvements based on lessons learned
Create Integrative Communication Mechanism	• Create a Task Force (e.g., “Fusion Center”) of Field Reps with a protocol for the regional office to establish communication channels
Clarify Responsibilities	• Inform stakeholders of who is responsible for what, with a single-entry point for communications • Improve tactical delineation of lines of effort, with clear responsibilities defined
Leverage Existing Infrastructure	• Utilize DHS Fusion Centers and FBI Field Offices • Provide training to Fusion Center Field Reps on the specific information to obtain for a cyber incident
Build Trust & Cooperation	• Improve agency image with industry by acknowledging industry competition as valid and aligning with cooperative goals
Develop Exercises Based on Prospective Threats	• Conduct “foresight” exercises to address the challenge of ever-changing technology landscape, rather than looking to the past for lessons learned

Table 2 Enhance Processes for Implementing Lessons Learned Thematic Responses

Q2. Increase Private Sector Involvement in Threat Response

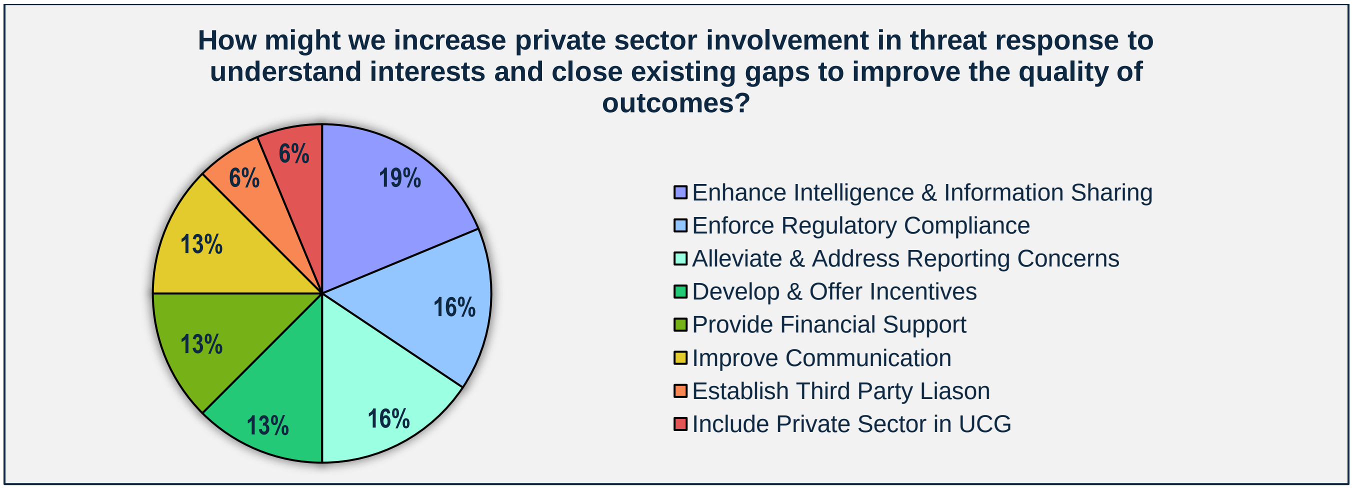


Figure 7 Private Sector Involvement Solution Set Themes

SOLUTION SET" CATEGORY	SAMPLE RESPONSES
Enhance Intelligence & Information Sharing	• Formulate key intelligence questions with the private sector • Increase utilization of the Joint Cyber Defense Collaborative (JCDC) • Promote timely declassification of intel for sharing with the private sector
Enforce Regulatory Compliance	• Enforce consequences for non-compliance with regulations • Enhance cooperation between victims and law enforcement • Foster joint government/private development of industry standards
Alleviate & Address Reporting Concerns	• Enhance community outreach and education • Address insurance-related reporting concerns • Mitigate potential punitive actions against private sector for sharing with regulators • Reduce the chilling effect of sharing info with SRMA and regulatory agencies
Develop & Offer Incentives	• Create incentive programs for industry to report cyber incidents • Offer incentives to industry (e.g., Safety Act, CTPAT Trade Compliance, Global Entry) • Facilitate bulk purchase of private sector intel for interagency use
Provide Financial Support	• Provide government assistance to industry for problem-solving and defense improvement • Discuss investment levels with the industry and communicate the cost of incident response and mitigation to the private sector
Improve Communication	• Encourage the private sector to voice their concerns and suggestions • Utilize the CISO Academy to educate Chief Information Security Officers about the roles and responsibilities of federal partners • Share information to improve ongoing relationships
Establish Third Party Liaison	• Create a non-regulatory intermediary to engage with the industry in cybersecurity • Use SRMAs as an information conduit to and from the sector
Include Private Sector in UCG	• Increase private sector involvement in the UCG process • Provide access to a classified UCG for cleared industry partners as needed

Table 3 Private Sector Involvement Thematic Responses

Q3. Ensure Readily Available Tools/Processes

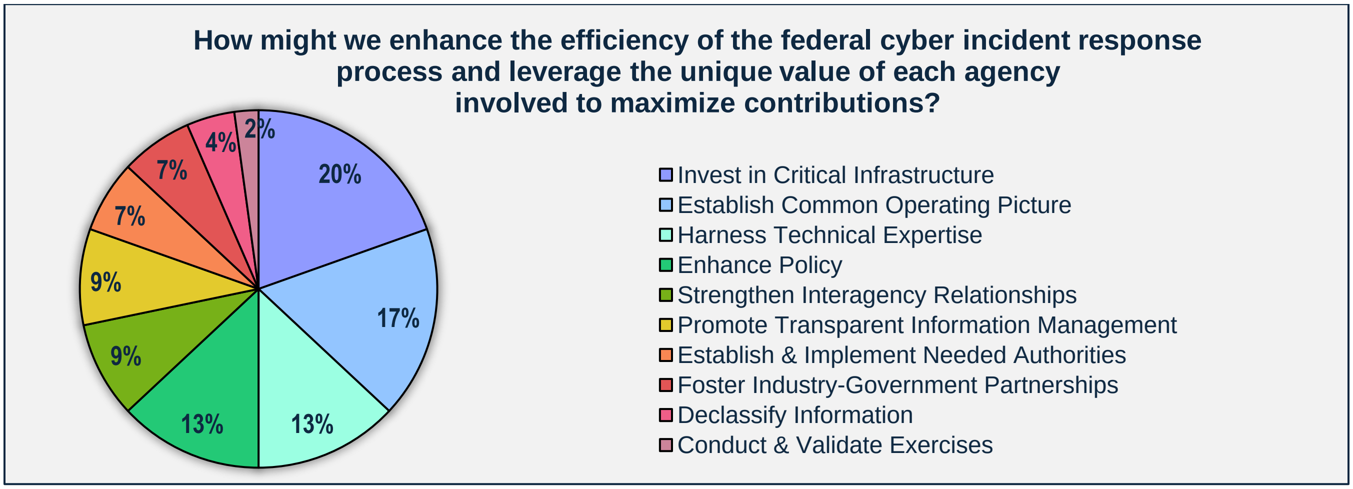


Figure 8 Tools/Processes Solution Set Themes

"SOLUTION SET" CATEGORY	SAMPLE RESPONSES
Invest in Critical Infrastructure	• Ensure clear communication to Congress about necessary resources • Provision grant opportunities to smaller entities • Assure fully funded grant programs accessible by critical infrastructure owners/operators
Establish Common Operating Picture	• Improve understanding of inter- and intra-agency logistics in response • Create a multi-level common operating picture
Harness Technical Expertise	• Draw on technical expertise, intelligence, tools, and data availability through identifying appropriate agency contacts
Enhance Policy	• Rewrite PPD-21 • Link to international resources/learnings • Use lessons learned from past incident responses to incidents for policy updates
Strengthen Interagency Relationships	• Address interagency challenges to data availability by promoting and continuing to develop relationships
Promote Transparent Information Management	• Encourage and increase interagency information sharing • Promote honest reporting up the chain
Establish & Implement Needed Authorities	• Secure legislative/regulatory authority to receive data reflecting operational disruptions to service delivery • Pursue enhanced authorities and ability to exercise those authorities
Foster Industry-Government Partnerships	• Enhance victim cooperation via an industry/federal employee planned rotation program • Increase information-sharing between the private sector and the UCG
Declassify Information	• Reduce intel classification and facilitate declassification
Conduct & Validate Exercises	• Conduct targeted tabletop exercises to inform plan requirements and determine tools needed for effective response

Table 4 Tools/Processes Thematic Responses

Q4. Enhance Process Efficiency and Maximize Contributions

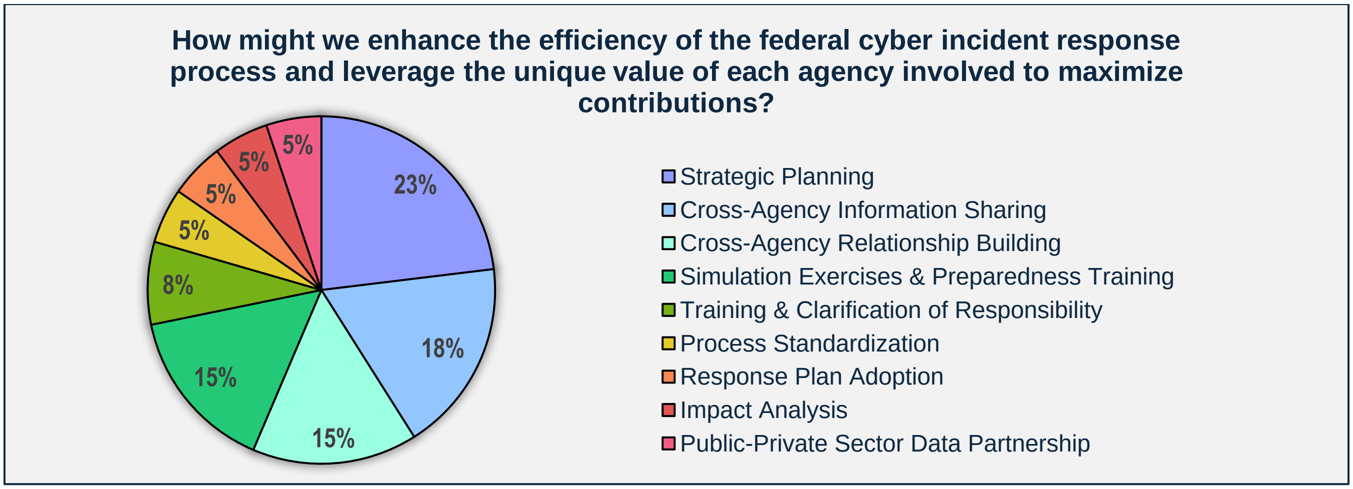


Figure 9 Process Efficiency and Maximizing Contributions Solution Set Themes

“SOLUTION SET” CATEGORY	SAMPLE RESPONSES
Strategic Planning	• Standardize SRMA activities across the U.S. government and create action plans • Learn more about the standard procedures at other agencies • Prepare a list of UCG participants prior to an incident
Cross-Agency Information Sharing	• Ensure each agency shares information, designating information to the lowest possible classification • Simplify the process of requesting and providing information • Use existing coordination pathways
Cross-Agency Relationship Building	• Rebuild a strong policy committee • Decide who should regularly attend SRMAs
Simulation Exercises & Preparedness Training	• Organize practice exercises with senior leaders and line-level staff • Conduct cyber-specific exercises at the regional level with federal involvement
Training & Clarification of Responsibilities	• Establish a clear understanding of the UCG structure and its participants • Conduct training for UCG operations
Process Standardization	• Establish repeatable process/playbook for SRMA use
Response Plan Adoption	• Ensure adoption of the National Cyber Incident Response Plans
Impact Analysis	• Create mechanisms for information sharing among different programs and agencies working on supply chain issues
Public-Private Sector Data Partnerships	• Share private incident response data among government agencies

Table 5 Process Efficiency and Maximizing Contributions Thematic Responses

Q5. Leverage Economic Insights and Data for Decision-Making

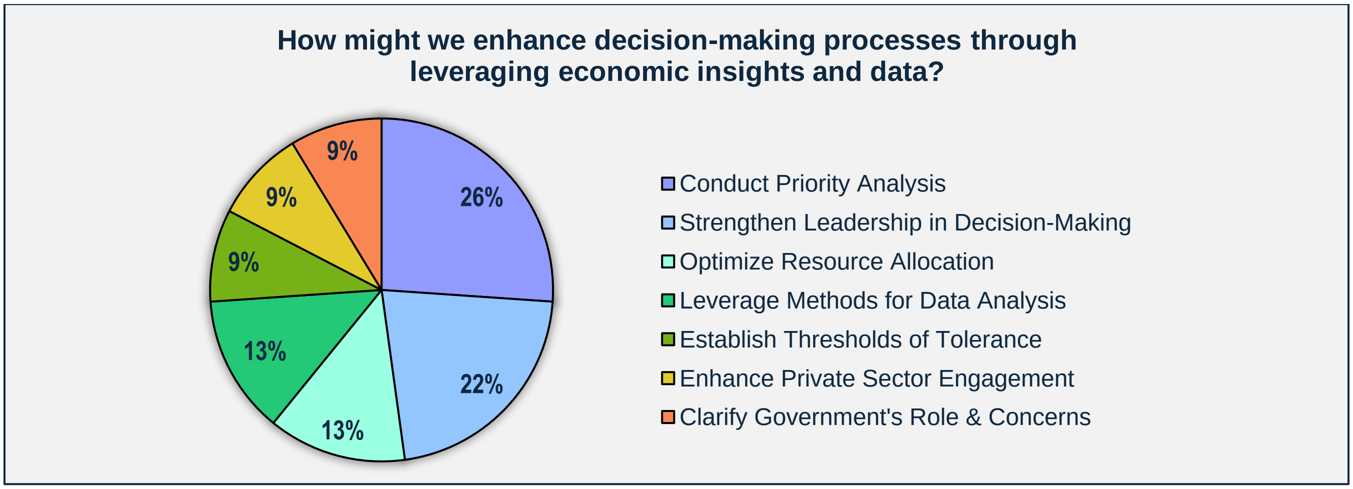


Figure 10 Economic Insights and Data for Decision-Making Solution Set Themes

"SOLUTION SET" CATEGORY	SAMPLE RESPONSES
Conduct Priority Analysis	• Devise unified strategy based on critical commodities for prioritizing goods after a prolonged downtime (reconciling opposing priorities, considering the immediacy and long-term effects of safety issues) • Apply strategic frameworks such as: ○ Political, Military, Economic, Social, Information, Infrastructure, Physical environment & Time (PMESII-PT); and ○ Diplomatic, informational, military, economic, financial, intelligence, & law enforcement (DIME-FIL).
Strengthen Leadership in Decision-Making	• Identify key decision-makers for economic recovery initiatives • Determine leadership authorities for prioritization decisions
Optimize Resource Allocation	• Leverage lessons learned COVID-19 pandemic national stockpile management • Develop tools for balancing "just-in-time" logistics & stockpiling/pre-positioning strategies • Develop Time-Phased Force Deployment Data (TPFDDs) for cyber-disruption response
Leverage Methods for Data Analysis	• Advance data protection methods for aggregated economic data supporting disruption response • Evaluate the importance and economic impact of insights • Apply techniques such as qualitative analysis, text/sentiment analysis, & large-language models
Establish Thresholds of Tolerance	• Determine metrics for evaluating threat severity (e.g., monetary, cross-sector impacts, and life safety/health) • Identify specific metrics for situational shift from a homeland issue to a national security concern
Enhance Private Sector Engagement	• Engage with private sector to enhance decision-making processes • Consider proprietary nature of carriers and their reluctance to share economic impact data
Clarify Government's Role & Concerns	• Leverage congressional relationships to learn more about constituency needs in targeted sectors/economic concerns • Promote interagency understanding of the specific roles of their counterparts

Table 6 Economic Insights and Data for Decision-Making Thematic Responses

Opportunities

Analysis Methodology

From the interviews and convening exercises in Phase 1, MITRE captured, collected, and sorted a substantial amount of qualitative data. MITRE determined a thematic analysis to be the best approach in examining data collected and identifying common themes, topics, and ideas that describe challenges and opportunity areas foundational to working towards advancing solutions. The analysis involved the following steps:

- ***Familiarization: Identifying what, where and how the data was derived.*** The analysis team sorted through the collection of data and identified what key points and topic areas were specific to each stakeholder and equities represented during interviews and convening exercises.
- ***Coding: Aggregating and classifying the data.*** The analysis team coded, arranged, and classified the data into categories by identifying similar attributes and information derived from the data.
- ***Defining: Naming the themes.*** Collectively, the team named the categories for each dataset as overarching themes that signify key issues and challenges derived from the data collected. The themes were subsequently organized into broad Challenge Areas.
- ***Reviewing: Validating the analytic process.*** Finally, the analysis team leveraged subject matter experts to validate the approach to data collection, categorization, and outcomes leading to the identified challenges and opportunities. The challenge areas and themes were refined and aligned to a set of potential solutions and approaches, providing a strategic framework for addressing the challenge space (Figure 11).

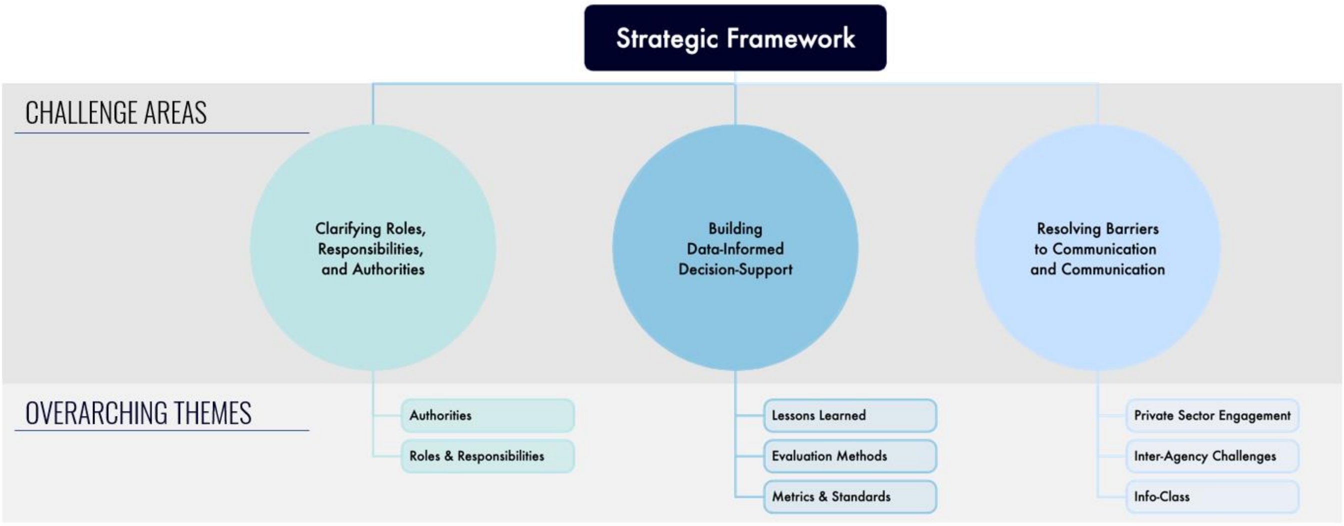


Figure 11 Strategic Framework

The following section summarizes the opportunities identified within the Challenge Areas of the Strategic Framework, as well as the Overarching Themes and corresponding actions that were identified and discussed as possible steps toward addressing the challenges identified in the research, interviews, and convening.

Clarifying Roles, Responsibilities, and Authorities

The opportunities in this section are derived from the overarching themes of "Authorities" and "Roles & Responsibilities." The Authorities theme refers to the power to implement or enforce policies. Participants highlighted the need to clarify these authorities, suggesting the mapping of authorities and procedures of federal programs and directives. The Roles & Responsibilities theme refers to the tasks and duties assigned to different entities. Participants emphasized the need for tactical delineation of lines of effort with clear responsibilities defined, which could be addressed by developing a Unified Response Playbook. As a result, the following opportunities for improvement were identified:

- Map authorities and procedures of federal programs and directives to mitigate confusion across policies/directive.
- Develop Unified Response Playbook to create common understanding of UCG policies and procedures.

Building Data-Informed Decision Support

The opportunities in this section are derived from the overarching themes of "Lessons Learned," "Evaluation Methods," and "Metrics & Standards."

Within the Lessons Learned theme, which encompasses the practices of documenting and implementing insights from past experiences, participants underscored the importance of formal, systematic documentation and implementation of lessons learned. Participants' responses highlighted the need for an information architecture that can enable tracking trends over time, from both real-life and simulated events, to enhance the efficiency and effectiveness of incident response. This could involve maintaining a central repository of learning from exercises across agencies and making lessons learned accessible to all.

The Evaluation Methods theme primarily refers to the establishment of systemic ways to assess the prioritization of response operations. Participants highlighted the importance of partnerships among agencies for leveraging existing tools and data to develop commodity prioritization modeling capabilities and a decision framework.

The Metrics & Standards theme refers to the creation and application of consistent measures and guidelines. Discussions revealed the need for a standardized process for assessing the severity of threats and determining specific thresholds for escalating the response to transportation disruptions. This might involve establishing thresholds of tolerance to determine acceptable levels of disruption. Additionally, conducting third-party evaluations of critical response efforts to real-life events was suggested to inform updates to standard operating procedures.

Based on participants' responses in these exercises, the following opportunities were identified:

- Create an information architecture to inform updates and document lessons learned from real-life and simulation events to track trends over time.
- Develop a standardized process for assessing risk and escalation in response to transportation disruptions.
- Conduct third-party evaluations of critical response to real-life events to inform updates of standard operating procedures.
- Partner among agencies, drawing on existing tools such as USDOT's FLOW and CBP, to develop a commodity prioritization modeling and decision framework, integrating commercial solutions, as appropriate.

Resolving Barriers to Effective Communication & Collaboration

The opportunities in this section are derived from the overarching themes of “Private Sector Engagement”, “Inter-Agency Challenges,” and “Information Classification (Info-Class).”

The Private Sector Engagement theme refers to the interactions and relationships between government entities and private sector organizations. Participants suggested the need for building trust and cooperation, providing financial support, and improving communication with the private sector.

The Inter-Agency Challenges theme refers to the difficulties in coordinating and collaborating across different agencies. Participants pointed out the high turnover of personnel as a challenge to maintaining relationships and continuity and indicated the need for a standing interagency task force to address this challenge.

The Information Classification theme primarily involves the complexities surrounding classification of intelligence information among agencies. The discussion revealed the need for interagency information sharing and increased communication, suggesting a study into the challenges of information classification and its impacts on sharing.

Based on participants' responses in these exercises, the following opportunities were identified:

- Host regular “red team” conference of government/industry emergency response coordinators and leaders.
- Study challenges of information classification and its impacts on sharing (e.g., over classification, industry clearance) and advance solutions, such as developing a new framework to guide future handling.
- Study the need for a standing interagency task force to respond to transportation disruptions rapidly and efficiently.

Looking Ahead

While all levels of government and the transportation industry have critical roles in the response to a national scale disruption to the U.S. transportation network, this initial review was organized to learn about federal needs, priorities, and challenges. As the project progresses, Phase 2 will expand to include and seek input from other parties. Convenings will continue to be structured to maximize collaboration, sense making, idea generation, and action taking to advance comprehensive solutions to critical challenges faced in mounting a unified response to national disruptions.

Appendix A

The following scenario was provided to participants at the March 20, 2024, convening to lay the foundation to jointly explore processes, pain points, and challenges associated with the federal response to a national transportation disruption viewed through the lens of a concerted cyber campaign—beginning with cyber-attacks on two key components of rail infrastructure, followed by a cyber-attack on a pipeline.

1. SCENARIO

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Cyber Attack on the Rail System

In an unprecedented cyber-attack, the Belt Railway Company of Chicago and Kansas City Terminal Railway (KCTR) face severe disruptions, bringing the national rail infrastructure to a standstill and prompting swift government intervention.

The Belt Railway Company of Chicago experiences a sudden and unexplained disruption in its operations. The computer aided dispatch servers begin to exhibit intermittent outages. As a result, Belt Railway stops movement of freight locomotives in its operating region, forcing major Class I freight companies, which rely on Belt Railway for interchange operations, to seek alternative routes or locations for transcontinental product movement. Local passenger/commuter traffic in the Chicago area is also stopped.

Later that day, the Positive Train Control (PTC) systems at KCTR unexpectedly go offline. As a legal measure, KCTR immediately halts all trains and operations. This results in trains across the network coming to a standstill, exacerbating shipping delays and congestion already impacting intermodal transfers from west coast ports.

As these events unfold, the Intelligence Community, which has been actively tracking a specific Advanced Persistent Threat (APT) using Signals Intelligence (SIGINT) and Human Intelligence (HUMINT), identifies patterns consistent with this APT's known tactics, techniques, and procedures. They quickly attribute the disruptions at the Belt Railway and KCTR to a cyber-attack by this known adversary. Despite their foreknowledge of the threat, they were unable to prevent the attack.

The government responds swiftly, forming a Unified Coordination Group (UCG) by the end of the day to coordinate the response to this significant cyber-attack on the national rail infrastructure.

Technology

Dispatch servers are computer systems that control train schedules and signals to prevent collisions. As the central hub of railway operations, dispatch servers process real-time data on each train's location, speed, and direction to ensure safe, efficient, and timely train operations.

PTC systems are safety mechanisms aimed at averting train accidents. Adding an extra layer of safety to train operations, PTC systems oversee train operations and autonomously decelerate or halt trains at risk of collision, derailment from high speed, or entering maintenance zones.

As of 2023, trains may only operate on PTC-mandated territory without a functioning PTC system if the system fails while on route. In these instances, they are permitted to continue operation with speed limitations until they reach a designated location for PTC repair (Title 49 CFR Sections 236.567 and/or 236.1029).

Belt Railway & KCTR Significance

The Belt Railway is the largest intermediate switching terminal railroad in the U.S. It is co-owned by six Class I railroads – BNSF Railway, Canadian National, Canadian Pacific, CSX, Norfolk Southern, and Union Pacific, each of which uses the company's switching and interchange facilities.

KCTR, based in Kansas City, operates under five Class I owners - Union Pacific, BNSF Railway, Kansas City Southern, Norfolk Southern, and Canadian Pacific. Kansas City is the second largest rail hub in the U.S., serving as an alternative route to bypass congestion in Chicago.

The Belt Railway and KCTR are critical to the "Transportation Services" National Critical Function (NCF). This function ensures the safe and efficient movement of people and goods across the U.S.

Freight Rail Commodity Flows

With one-third of the nation's rail freight capacity transported through Chicago and Kansas City (Figure 1), rail congestion in these cities has a significant impact on commodity flows across the country. This is particularly true for the transportation of "Chemicals or Allied Products", which represents a substantial portion of the total shipments (Figure 2). Chemical products, including industrial chemicals, pharmaceuticals and more, are vital to various economic sectors. Any disruption to the flow of chemical products will therefore have far-reaching consequences, going beyond the chemical industry to all dependent and interdependent sectors.

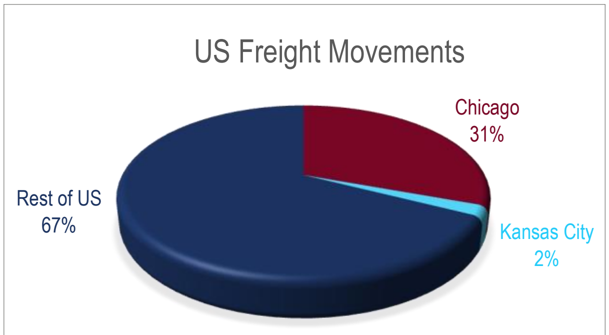


Figure 1. Developed from Public Waybill Data (Surface Transportation Board) 2021 (Chicago & Kansas BEA)

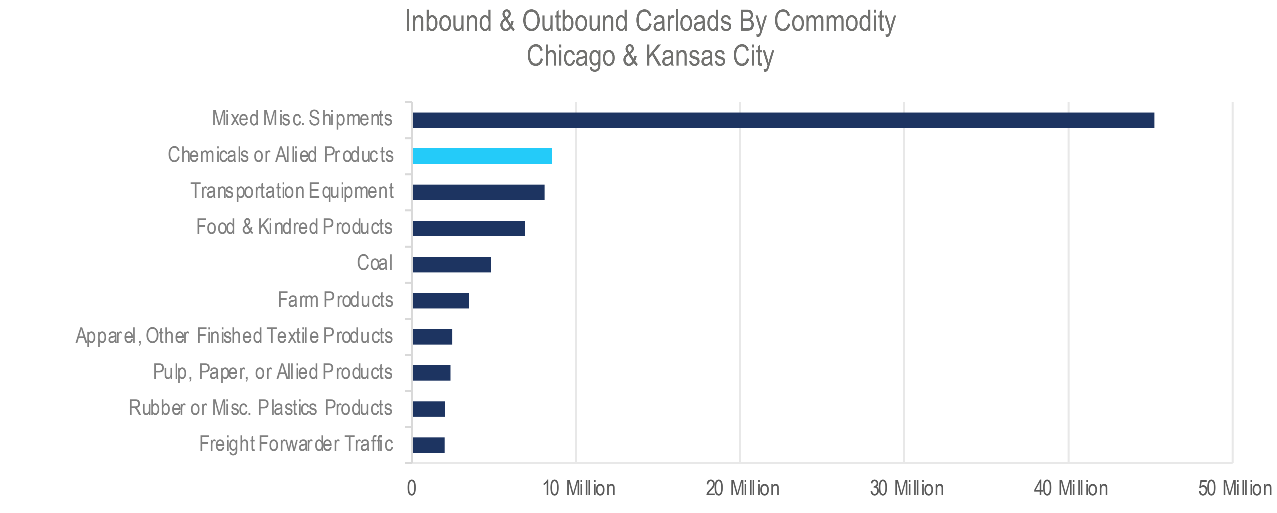


Figure 2. Developed from Public Waybill Data (Surface Transportation Board) 2021 (Chicago & Kansas BEA)

1.2. COMMODITIES

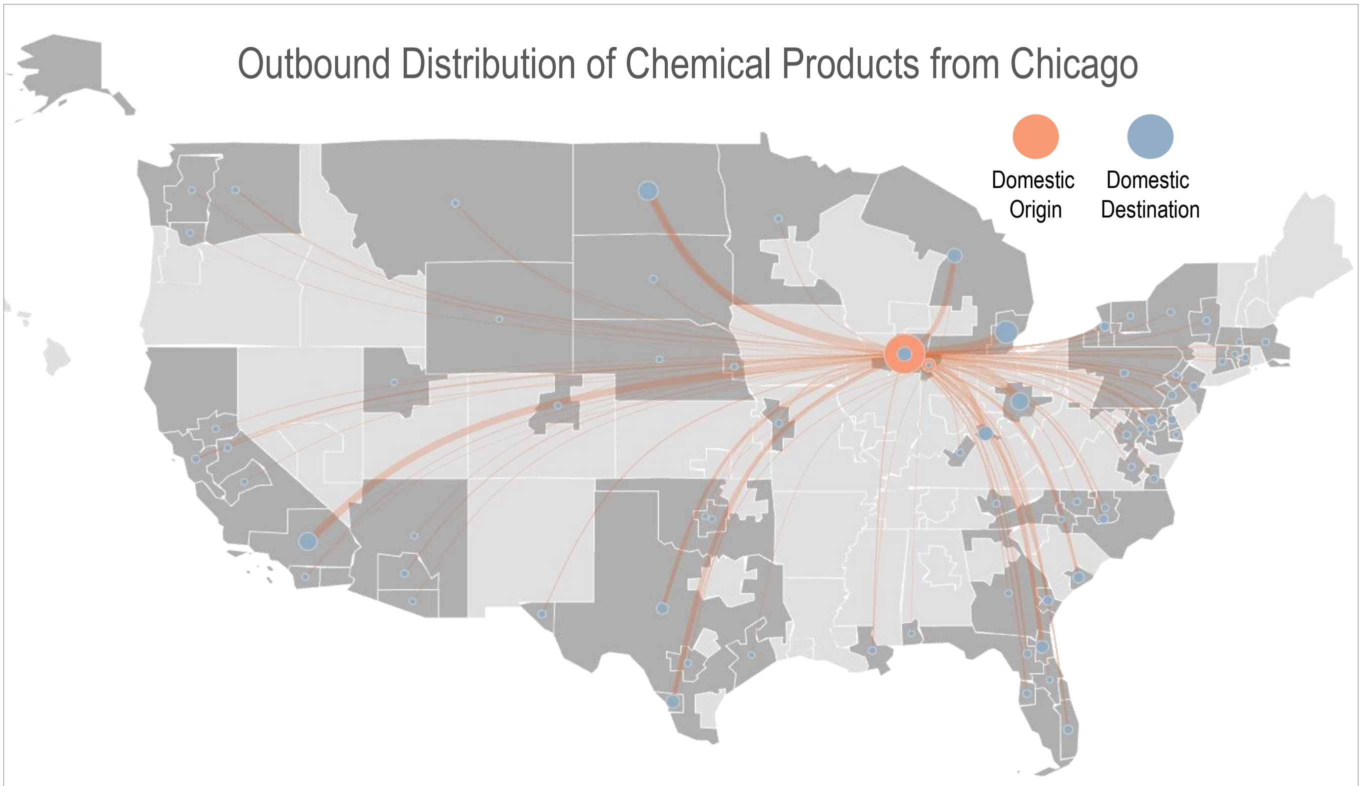


Figure 3. Visualization created using Data Tabulation Tool (DTT) web-based interface using Freight Analysis Framework Version 5 (FAF5) data set for 'Total Flows' of commodities by rail. FAF Zones: 171, 181; CFS Area: 17-176, 18-176. https://faf.ornl.gov/faf5/dtt_total.aspx

The outbound distribution of chemicals products from Chicago demonstrates the complex web of dependencies and interdependencies within rail infrastructure (Figure 3).

The uninterrupted flow of chemical products is vital for fulfilling mission-critical functions, or NCFs. Delays in shipping these critical commodities can pose significant risks to key NCFs such as energy, agriculture, and manufacturing. The table below demonstrates the reliance of various NCFs on chemical products:

National Critical Functions: Reliance on Chemical Products

Healthcare	Food & Agriculture	Energy	Water & Wastewater	Transportation Systems	Manufacturing	Information Technology	Emergency Services
Production of pharmaceutical, medical supplies & medical equipment.	Fertilizers, pesticides, food preservatives, food processing & packaging.	Fuel production, power plant operations, manufacturing of solar panels and batteries, oil & gas extraction & refining.	Water treatment processes for safe drinking water & wastewater treatment.	Production and maintenance of vehicles, roads, and rail tracks, fuels & lubricants for transport.	Production of plastics, textiles, electronics, machinery.	Production of hardware components, batteries, and other IT equipment.	Firefighting foams, emergency medical supplies, hazardous material response equipment.

1.2. COMMODITIES

Hazardous Materials

Chemical and allied products encompass a wide variety of items, many of which are classified as hazardous materials. Nearly half of these chemical products are classified as hazardous materials (Figure 4), requiring special handling and transportation protocols to ensure safety and mitigate environmental risks.

Given these constraints, rail is the primary mode of transportation for hazardous materials. Safety protocols, stringent regulations, and robust emergency response plans make rail transport a safer option for hazardous materials, reducing the risk of accidents compared to other modes of transportation. Rail transport ensures hazardous materials are properly stored and handled, thereby minimizing public health and safety risks.

According to the regional breakdown by the Bureau of Economic Analysis (BEA), which is based on factors like economic ties and commuting patterns, (Figure 5), the Chicago region is responsible for approximately 22% of all outbound hazardous materials transported by rail. This is a substantial proportion compared to the other 92 regions.

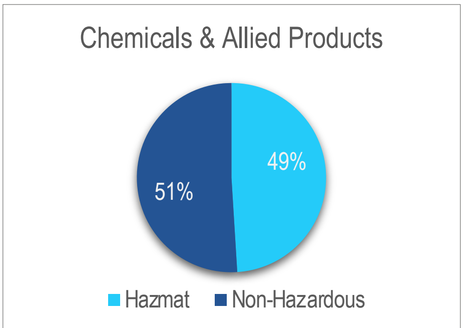


Figure 4. Developed from Public Waybill Data (Surface Transportation Board) 2021 (Chicago & Kansas BEA)

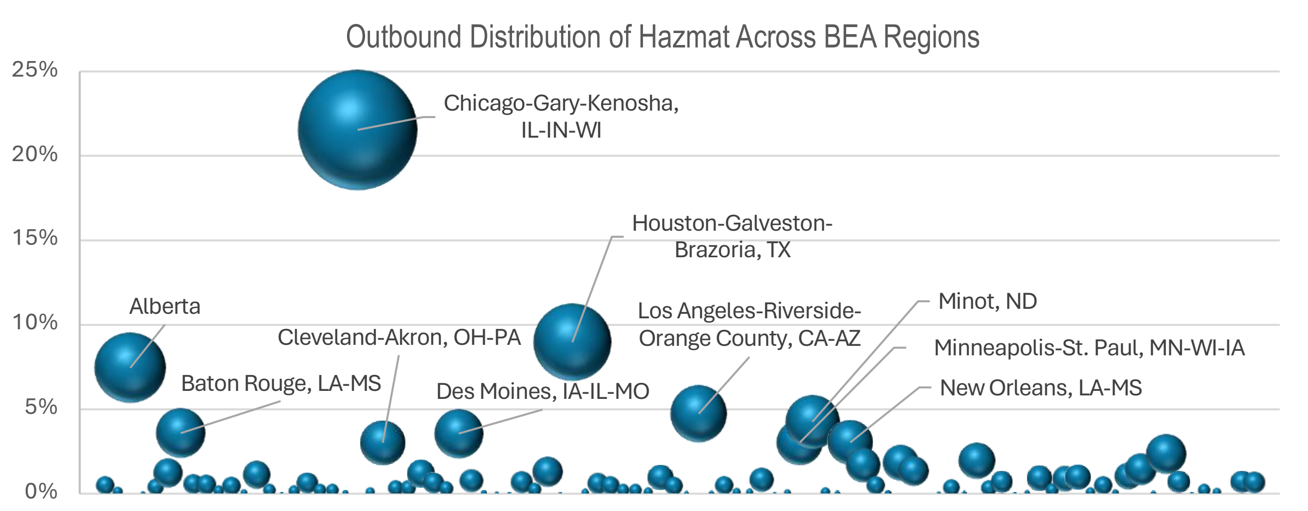


Figure 5. Developed from Public Waybill Data (Surface Transportation Board) 2021 (Chicago & Kansas BEA)

Chlorine & Anhydrous Ammonia

Chlorine and anhydrous ammonia are key hazardous materials transported by rail. Their importance lies in their widespread use in various industries, making them integral to the U.S. economy. However, these substances are also categorized as Toxic Inhalation Hazards (TIH) due to the substantial health risks they pose if released into the atmosphere. Despite the associated risks, these substances provide significant economic benefits.

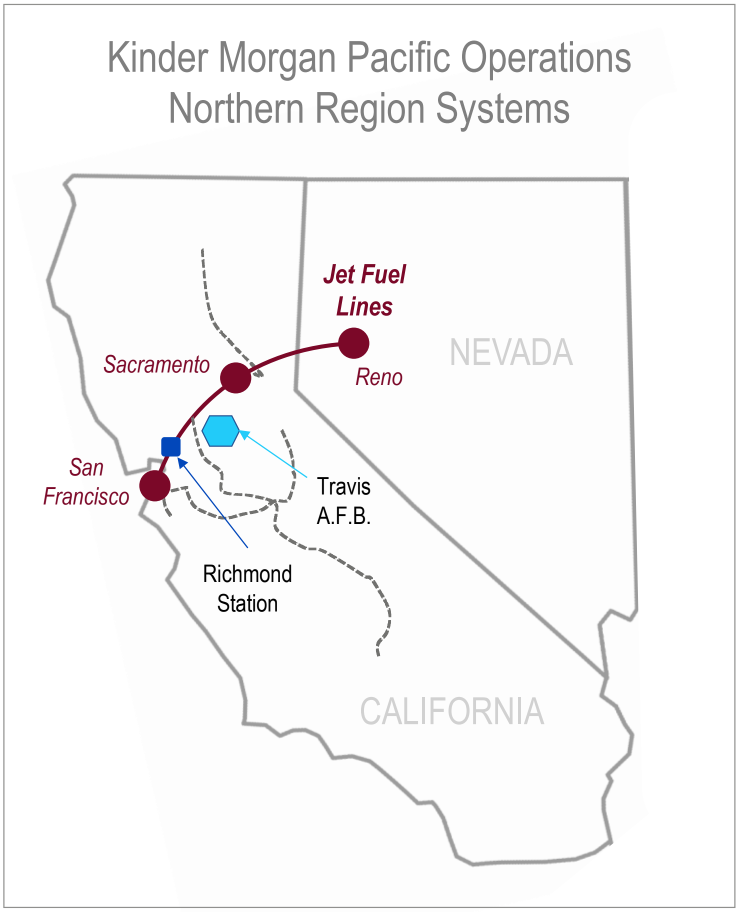
The absence of Chlorine and Anhydrous Ammonia could lead to significant disruptions, such as the closure of gas stations, reduced crop yields, increased potable water prices, and a halt in many manufacturing activities. For instance, chlorine gas is used nationwide for purifying potable and wastewater at treatment plants and as a chemical intermediary in the manufacturing of various products, from PVC pipes to shampoo. An estimated 85% of long-distance chlorine transportation occurs by rail. Anhydrous ammonia, the nation's primary commercial fertilizer, is extensively used across the country's main agricultural regions, especially in the Midwest farm states.

2. INJECT ONE

Pipeline Cyber Attack

A day after the cyber-attacks on the Belt Railway and KCTR, cyber actors target the Pacific Operations Northern Region of the Kinder Morgan pipeline. Richmond station, a vital node in the pipeline network responsible for delivering jet fuel to various locations including Travis Air Force Base and surrounding airports, is hit with Ransomware. The malicious software infiltrates the IT systems and spreads to a gas compressor station, compromising the operational integrity of the pipeline. Adding to the chaos, false leak detection alerts are triggered at select locations downstream of the Richmond station. These alerts raise fears of potential environmental damage and safety concerns.

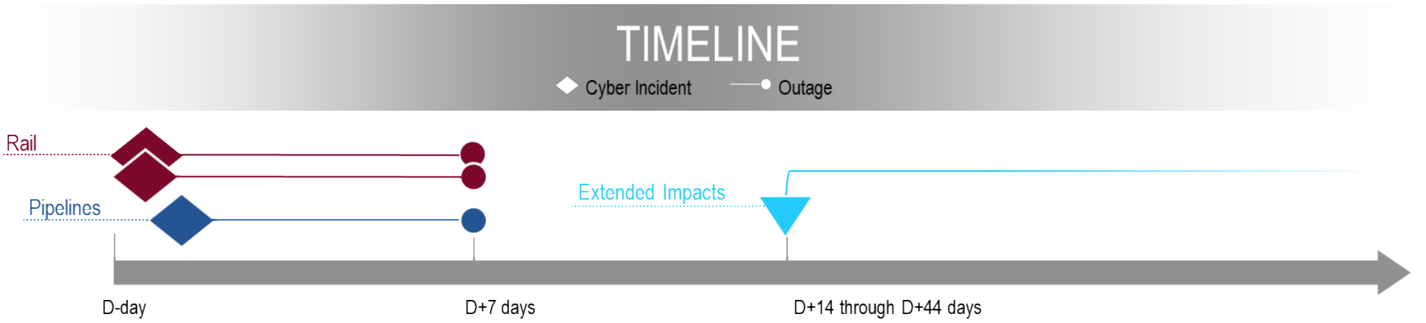
Kinder Morgan is forced to shut down pipeline operations to restore the affected systems from backup. This immediate halt in operations disrupts the flow of jet fuel, causing significant concerns regarding the operational readiness of military bases and the continuity of commercial air services in the region.



In the wake of these attacks, the Intelligence Community intensifies its investigation. Leveraging their SIGINT and HUMINT capabilities, they uncover evidence that the disruptions at the Belt Railway, KCTR, and Kinder Morgan pipeline were not isolated incidents but part of a concerted cyber campaign.

The government responds by expanding the mandate of the Unified Coordination Group (UCG) to include the pipeline attack. The UCG now faces the daunting task of coordinating the response to two major cyber attacks on critical infrastructure, further complicating the recovery process and highlighting the urgent need for enhanced cybersecurity measures.

3. INJECT TWO



Severity of Impacts

Rail Congestion Accelerates. In the aftermath of the cyber attacks on rail infrastructure, the simultaneous unavailability of both KCTR and the Belt Railway brings both passenger and freight rail networks to a standstill. The affected railroads are eager to restart operations, but they are hesitant while restoring IT system functionality and seeking a waiver of PTC regulation from Federal Railroad Administration (FRA). Concerned about the potential for further disruptions and compromised operational performance, Belt Railway and KCTR opt to wait until they are confident the cyber threat has been fully neutralized.

The paralysis of the railroad network strains supply chains and reverberates across sectors. Industries ranging from manufacturing to retail grapple with shipping delays greater than 30 days and an inability to receive and ship commodities such as chlorine for water treatment facilities and anhydrous ammonia for Midwest farm states. Congestion accelerates, impacting intermodal transfers and leading to increased dwell times.

Fuel Shortages. With halted operations at the Richmond station, the jet fuel shortage begins to severely impact both commercial and military aviation. Travis Air Force Base is forced to limit non-essential operations, affecting military readiness and causing delays in troop and equipment transportation. Commercial airlines serving the affected airports begin to experience significant disruptions. As a result, a large number of flights are cancelled or delayed, and thousands of passengers are stranded or forced to alter their travel plans. The airlines start to incur heavy financial losses due to refunds, rerouting passengers, and damage to their reputation.

The effects of the fuel shortage cascades to other industries. Logistics companies that rely on air freight for timely delivery of goods face significant delays. This impacts industries such as e-commerce, manufacturing, and pharmaceuticals, where timely delivery is crucial.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

For more information, contact:

resilientransport@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®