Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation

September 2015
Foreword

In the days, months, and years following the events of September 11, AASHTO and its partners united through the Transportation Research Board to improve and enhance the skills of the transportation community to prepare for and respond to events of terrorism that threaten the transportation system. One of many products produced was a Guide to Understanding the Fundamentals of Effective Security Management. In the intervening years it has become clear that the learning achieved not only applied to security threats but to all forms of threats to the transportation system.

Today we understand that:

- **Customers today have higher expectations for system performance and reliability and lower tolerance for delays.** Even small events pose threats of great consequences since the impact of any incident is magnified.
- **Hazards continue to evolve. Extreme weather, cyber incidents, and other additional hazards need to be addressed.** In addition, the risk of natural and man-made events is growing more common due to many pressures, including an aging infrastructure.
- **Today’s transportation systems are integrated cyber and physical systems.** There has been, and continues to be, significant deployment of new technologies to support DOT activities.

This newly updated Fundamentals Guide synthesizes the most recent federal and state guidance and research efforts from a state DOT perspective and lays out a set of capabilities for state DOTs that addresses all-hazards infrastructure protection, resilience, and emergency management and reflects National Preparedness Goals. The goal of the Guide is to provide a resource for state DOTs that supports the integration of infrastructure protection and resilience into all of their operations and infrastructure programs.

To ensure the security and resilience of our nation’s transportation systems, AASHTO member DOTs, along with local, state, and federal emergency response agencies have become strong security and emergency response partners. This Fundamentals Guide provides you the best and latest thinking on how to remain the best at what we do and how we can remain that way moving further into the 21st Century. This Guide and our partnerships will help to keep the nation’s transportation system strong and well protected no matter what the event that may threaten it.

John Cox
Director
Wyoming Department of Transportation
2015 AASHTO President

Brian Ness
Director
Idaho Transportation Department
Chair, AASHTO Special Committee on Transportation Security and Emergency Management
Preface

This guide is an update to the 2007 Fundamentals of Effective All Hazards Security Management for State DOTs. The original guide was intended to provide DOT managers with an overview of an effective all-hazards security management program. It outlined the fundamental responsibilities of a state department of transportation (DOT):

1. Prevent incidents within their control and responsibility;
2. Protect transportation users, agency personnel, and critical infrastructure;
3. Support regional/state/local emergency responders with resources including facilities, equipment, and personnel;
4. Recover swiftly from incidents;
5. Evaluate response(s) and continually improve plans, training, skills, and protocols.

Since the time of that publication, the fundamental responsibilities of DOTs have not significantly changed but the capabilities necessary to perform those responsibilities have evolved. AASHTO has recognized five “fundamentals” documents, most published since 2009, that provide comprehensive guidance on the major elements of a state DOT all-hazards transportation security and emergency management program:


Since 2010, four significant national-level directives and executive orders have been issued:

- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013) focuses on the need for secure critical infrastructure that is able to withstand and rapidly recover from all hazards (resilient).
- National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience emphasizes the importance of resilience, and the need to reduce all-hazards vulnerabilities and mitigate potential consequences of incidents or events that do occur.
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013) provides a technology-neutral cybersecurity framework and means to promote the adoption of cybersecurity practices.
Table of Contents

Foreword .......................... 1
Preface ................................ 3
Introduction .......................... 7
Summary of Fundamental Capabilities .................................................. 11
Planning .................................. 13
Public Information .................... 17
Operational Coordination .......... 21
Prevention ............................... 25
Protection ............................... 29
Mitigation ............................... 33
Response .................................. 37
Recovery .................................. 41
Cybersecurity ............................ 43
Training and Exercises ............ 49
Appendix A: Selected References . 51
Appendix B: Definitions ............. 53
Appendix C: Acronyms ................. 67
Introduction

Evolving DOT priorities, research on security and emergency management, and new federal guidance issued since 2010 have prompted the need to re-examine DOT capabilities to support their fundamental roles. The 2007 version of the Fundamentals document focused on capabilities associated with security awareness, critical infrastructure/key asset protection, and readiness, response, and recovery. There is now an emerging focus on the complementary goals of infrastructure protection and resiliency as part of security and emergency management.

Figure 1. DOT Capabilities—2007 and Now

- **Customers today have higher expectations for system performance and reliability and lower tolerance for delays.** Even small events pose threats of great consequences since the impact of any incident is magnified when a transportation network is operating at or past its capacity—as is the case in portions of many states as travel demand on their transportation networks grows.

- **Hazards continue to evolve.** Extreme weather, cyber incidents, and other events need to be addressed. In addition, the risk of natural and man-made events is growing more common due to many pressures including aging infrastructure.

- **Today’s transportation systems are integrated cyber and physical systems.** There has been, and continues to be, significant deployment of new technologies to support DOT activities.

DOTs have a significant role in infrastructure protection. Transportation employees and contractors are the best positioned to know what is usual and unusual and can help their agency protect its employees, information, data, networks, and facilities. DOTs have the responsibility for controlling access to critical components, establishing coordination with law enforcement to ensure quick response to incidents, conducting risk and vulnerability
Resilience is “the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events” (Disaster Resilience: A National Imperative, National Research Council, 2012). DOTs are currently in the process of understanding the impact of the shift in focus from protection of assets to resilience of systems. In the context of transportation and infrastructure, the principles of resilience are shown in the box at right.

Overall DOT efforts have improved emergency response planning and training since the 2007 version of this Fundamentals document. When an emergency occurs, routine day-to-day operations give way to a focused, practiced, and resilient crisis management approach that requires professional skills throughout the breadth and depth of the organization. Traffic Incident Management (TIM) provides processes and procedures for responders (firefighters, emergency medical services, law enforcement, towing and recovery, safety patrols, transportation and maintenance crews, and 911 professionals) to work together as a team to clear incidents safely and quickly. The National Incident Management System (NIMS) integrates best practices into a comprehensive framework for use by emergency management personnel at the local, state, and federal levels. The Incident Command System (ICS) provides the integration of facilities, equipment, personnel, procedures, and communications for emergencies.
This 2015 Fundamentals document synthesizes the recent federal and state guidance and research efforts from a state DOT perspective and lays out a set of capabilities for state DOTs that addresses all-hazards infrastructure protection, resilience, and emergency management and reflects national preparedness goals. The goal of this document is to provide a resource for state DOTs that supports the integration of infrastructure protection and resilience into their operations and infrastructure programs.
Fundamental Capabilities of DOTs reflect an all-hazards approach including extreme weather, storm surges, natural events, accidental or unintended incidents, technological failure, and cybersecurity breach, and multi-modal risk assessment and management.

The capabilities reflect an all-hazards approach that includes a broad range of incidents and events that have potential to impact transportation systems operations. Extreme weather, cyber incidents, and other additional hazards need to be addressed as part of an all-hazards approach. Figure 2 includes the types and frequency of events that transportation agencies may encounter along with the other agencies (local, state, and federal) that may be involved depending on the severity or complexity of the incident.

The following sections provide a definition of each category, an overview of the key capabilities required for that category, and resources to support the implementation of those capabilities.

**Figure 2. Agency Involvement by Incident Level**

Source: NCHRP 525 Vol. 6, Security Guide for Emergency Transportation Operations
**Planning:** Conduct a systematic process that engages the whole regional community.

**Public Information and Warning:** Deliver coordinated, prompt, reliable, and actionable information.

**Operational Coordination:** Establish and maintain a unified and coordinated operational structure and process.

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Protection</th>
<th>Mitigation</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>To avoid, prevent, or stop a threatened or actual act of terrorism.</td>
<td>To secure against acts of terrorism and man-made or natural disasters.</td>
<td>To reduce loss of life and property by lessening the impact of disasters.</td>
<td>To save lives, protect property and the environment, and meet basic human needs after an incident has occurred.</td>
<td>To assist communities affected by an incident to recover effectively.</td>
</tr>
</tbody>
</table>

- Intelligence and information sharing
- Screening, search, and detection
- Access control
- Physical protective measures
- Risk management
- Supply chain integrity
- Long-term vulnerability reduction
- Risk and disaster resilience assessment
- Threat and hazard identification
- Critical transportation
- Operational communications
- Situational Assessment
- Infrastructure systems

**Cybersecurity:** Establish and maintain a cybersecurity program.

**Training and Exercises:** Prepare DOT employees for their roles

---

*Figure 3. Fundamental and Necessary Capabilities of State DOTs*
Conducting a systematic process that engages the whole regional community in the development of executable strategic, operational, and community-based approaches to meet defined objectives that are implementable using available resources and within the time constraints set forth by the agency.

As a part of their function, state DOTs are responsible for creating all-hazards plans and ensuring that employees have the ability to implement them. These all-hazards plans must conform with and complement the planning activities of the rest of the state’s operations and agencies as well as those of regional authorities. DOTs may coordinate planning efforts with other state agencies, including the state’s emergency management agency; county highway departments; various agencies of the U.S. DOT; and with DOTs from other states to ensure activities can be easily integrated when necessary. DOTs also need to plan to receive and use resources provided by other states and the federal government during operations. In conducting these planning activities, DOTs should consider applicable standards and best practices for incorporating risk and resilience into asset management functions and system design.

**Key Planning Capabilities**

- Use an all-hazards approach.
- Integrate security into planning.
- Ensure consistency with national planning programs.
- Coordinate planning for agency-wide consistency.
- Coordinate with regional partner plans and processes.
- Maintain support and participation from the top (critical).
- Ensure adequate distribution of plans.
- Review and update plans regularly.

The types of plans a DOT may create include:

- Infrastructure protection and security plans
- All-hazards mitigation plans
- Agency-wide emergency operations plan
- A continuity of operations (COOP) plan and COOP site whose capabilities are assessed on a regular basis
- Infrastructure and cybersecurity recovery/resiliency plans
- Communication plans

### Principles to Incorporate Security into Planning

- Risk-based designs
- Redundant components
- Support response
- Facilitate recovery
### Security Steps

**A. Security Advisory Team:** Have the team do a review at key steps in the planning process.

**B. Threat Assessment and Hazard Analysis**

**C. Threat and Hazard Mitigation Strategies**

**D. Incorporate Security Requirements**

**E. Develop Contract Language with Security in Mind**

**F. Conduct Security Reviews**

**G. Develop Scope of Work**

**H. Conduct Planning and Rehearsals**

### Transportation Planning Steps

1. **SYSTEM LEVEL ANALYSIS**
   - The local, state, and/or regional governing body determines the need for a new project in the area through a visioning exercise or needs assessment. Security: Steps: A

2. **PROJECT IDENTIFICATION**
   - More specific concepts like location, purpose, need, access, and funding sources are discussed. Security: Steps: B, C, D, F

3. **PROJECT PLANNING**
   - The regional planning process allows for a study of the proposed project area. The proposed project is reviewed and approved by the MPO for possible study in the Unified Planning Work Program (UPWP) and inclusion in the Long Range Transportation Plan (LRTP). Security: Steps: C, F

4. **PROJECT PROGRAMMING**
   - The project enters into the funding stage. The MPO will include the project in their Transportation Improvement Program (TIP). The state then adds the project to the Statewide Transportation Improvement Program (STIP) to ensure that transportation infrastructure funding is available for the project. Security: Steps: C, F

5. **PRELIMINARY DESIGN**
   - The project enters the preliminary design phase. The initial risk assessment and mitigation strategies are revisited to ensure security measures are incorporated into the design. Security: Steps: D, E, F, G, H

6. **ENVIRONMENTAL REVIEW**
   - The project now enters the project conformity and National Environmental Policy Act (NEPA) process to determine, minimize and if appropriate mitigate the project’s environmental impact. Security: Steps: D, F

7. **FINAL DESIGN**
   - The project design is approved with security considerations and environmental mitigation included. Final review of the risk assessment and mitigation strategies. Security: Steps: D, F, G

8. **ACQUISITION AND CONTRACTING**
   - Right of Way (ROW) acquisition
   - Acquisition of construction firm
   - Plan, Specification, and Estimate (PS&E) Agreement
   - Utilities
   - Security: Steps: F

9. **PROJECT CONSTRUCTION**
   - The project is constructed based on agreements and specifications from above steps. Security: Steps: A

10. **PROJECT ACCEPTANCE**
    - The Operator of the project will follow Standard Operating Procedures (SOP) to ensure safe and secure operation. Security: Steps: F, H

### Planning Techniques & Tips

**Broaden the Planning Team:** Incorporate non-traditional security partners early and often into the planning process to ensure quality input.

**Risk Management Program and Assessment:** Develop a Risk Management program and use it to evaluate the program and specific critical projects.

**Key Questions to Ask Early:**
1. Is the infrastructure critical?
2. What are the threats against the infrastructure?
3. How can design mitigate the threats?

**Conduct a Component Level Workshop:** Use this to establish the security requirements before the project moves to preliminary design.

**Critical Check Point:** These are the steps where security measures are incorporated into the project design. After this it becomes more expensive to add security elements.

**Standard Operating Procedures (SOPs):** Should be developed for both the construction and operations phases. Use the Security Advisory Team to ensure proper security considerations are incorporated.

**Environmental Review & Security Review Can Take Place Concurrently:** There may be inter-relationships between how the design incorporates both security and environmental elements.

---

**Figure 4.** Potential linkages to consider security in the project planning process. See the FHWA document to find suggested techniques and tips to help inform planning discussion about infrastructure protection and security.

Planning Resources

A guide developed by the U.S. Federal Highway Administration to help ensure that security and emergency management are considered during the planning phase of highway-related infrastructure projects. The intended audience is the transportation infrastructure project community, especially transportation planners at a state DOT or a regional metropolitan planning organization (MPO). The guide includes checklists, examples, and resources.

Integrating Security into the Project Planning and Development Process (2012)
This brochure outlines linkages for security planning into the project planning process and provides techniques and tips along with resources to help inform discussions about protection and security.

This guide provides an overview of high-level requirements for emergency response planning based on national policies, an agency self-assessment, and a resource guide with organization staffing guidance, decision-making sequences, and resource lists.

The guidelines were designed to assist transportation agencies in operations plans, policies, and procedures consistent with the National Incident Management System. Downloadable worksheets, template for a COOP plan, brochures to explain COOP planning process for staff, a customizable PowerPoint for executive leadership, and 300-plus resources organized in an electronic library are included.

http://transweb.sjsu.edu/project/1080.html
This report covers the research conducted to determine how to integrate COOP/COG into the overall NIMS approach to emergency management, including a connection between the emergency operations center (EOC) and the COOP/COG activity.

NCHRP Research Results Digest 333/TCRP Research Results Digest 90, Natural Hazards Informer Number 4, A Guide to Planning Resources on Transportation and Hazards (2009)
This joint NCHRP and TCRP report highlights a framework for thinking about the stages of a disaster and identifies some of the most current and innovative hazard-related research.
NIPP Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects (2013)
This DHS document report provides a summary of steps that support infrastructure development decisions and investments that will enhance the resilience of critical infrastructure systems.
Public Information

Delivering coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard and, as appropriate, the actions being taken and the assistance being made available.

Customers require timely and accurate travel information. Given the speed and frequency with which communication travels in today’s environment, communicating “regularly and often” may mean multiple times per day, especially during emergencies. As a public entity, the agency may be inundated with requests for public information. Demonstrating a commitment to honest transparency with information and public data can help build and maintain an agency’s reputation.

Key Public Information Capabilities

- Make sure that effective communications mechanisms and people are in place so that the agency can communicate regularly and competently to all stakeholders.
- Maintain clear and streamlined communications, with coordination and a cooperative attitude among all process stakeholders.
- Communicate regularly and often.
- Be proactive by releasing relevant and related public data.
- Leverage all appropriate communication means such as social media sites and web-based and mobile technology.
- Provide 24/7 travel information and timely alerts and warnings.
- Coordinate public information and establish procedures to ensure that DOT “speaks with one voice” and releases consistent information to the public and the media.
Figure 5. Communication Overlap with Transportation, Emergency Management, and Vulnerable Populations.

Figure 6. Agency Goals vs. Effectiveness of Social Media.
Source: TCRP Synthesis 99: Role of Social Media in Public Transportation (2012)
Public Information Resources

This guide describes how to create a communication process to reach vulnerable populations regarding their transportation options in emergencies. The toolkit provides a guiding framework and tools for constructing a scalable, adaptable communication process built on a network of agencies from public, private, and nonprofit sectors.

NCHRP Report 690: A Guidebook for Successful Communication, Cooperation, and Coordination Strategies between Transportation Agencies and Tribal Communities (2011)
This guidebook includes guidelines designed to help DOTs and tribal communities work together to achieve successful transportation projects on tribal lands. It offers a flexible approach that can be adapted to most situations and includes case studies to illustrate successful practices.

TCRP Synthesis 99: Uses of Social Media in Public Transportation (2012)
This report explores the use of social media among transit agencies and documents successful practices in the United States and Canada.
Operational Coordination

Establishing and maintaining a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

DOTs need to understand the specific procedures and protocols that have been established by other local, state, and federal agencies that may become involved with the DOT, especially those for managing incidents and emergencies. DOT staff should stay current regarding the applicable state and national standards for emergency preparedness and response. The federal government expects state DOTs to incorporate principles and concepts of national initiatives that provide common approaches to incident management and response in emergency response plans and operations. National initiatives include the National Response Framework (NRF) with its designated emergency support functions (ESFs) and the National Incident Management System (NIMS) with its protocols for multiagency interaction and communication. State and local NIMS compliance is a prerequisite for federal preparedness funds.

Key Operational Coordination Capabilities

- Establish internal state transportation agency communications protocols.
- Integrate and synchronize actions of participating organizations and jurisdictions to ensure unity of effort.
- Enhance and maintain NIMS-compliant command, control, and coordination structures to stabilize the incident and transition to recovery.
- Collaborate with all relevant local and regional partners.
- Establish clear lines and modes of communication among partner organizations and jurisdictions.
- Coordinate with appropriate local, regional, and national partners such as non-government organizations.
Figure 7. Regional Communication and Collaboration Circle of Principles.

Figure 8. Overview of National Incident Management System (NIMS) Coordination
Operational Coordination Resources


This guide specifies advance planning and collaboration principles to assist professionals in the transportation sector (all modes and across public, private, and nonprofit sectors) to facilitate informed dialogues and planning between transportation stakeholders and other major stakeholders for emergency planning. Its focus is to assist in the formation of grassroots collaborative networks to help plan ways to mitigate, respond to, and recover from emergencies, disasters, or significant events.

*National Incident Management System (NIMS) Training*


NIMS provide a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents. FEMA’s National Incident Management System Training offers a series of NIMS Courses that range from basic overviews to more advanced, position-specific training.

![Figure 9. Summary of FEMA NIMS Training Courses](image)

*Traffic Incident Management (TIM) Training*


SHRP2’s National Traffic Incident Management Responder Training brings DOTs, police, firefighters, towing, medical personnel, and other incident responders together to engage in interactive, hands-on incident resolution exercises.
Role of Transportation Management Centers in Emergency Operations Guidebook (2012)
This U.S. Federal Highway Administration guidebook covers ways to increase communication and collaboration between transportation management centers and emergency response agencies.
Avoiding, preventing, or stopping a threatened or actual act of terrorism.

Intelligence and information sharing is a major component of prevention. Because of their varied responsibilities and work locations, DOT employees are often the first to notice or learn about suspicious activity and are best positioned to recognize threats or security concerns to transportation systems. DOTs should encourage everyone to be aware of suspicious activity and know who to call to report matters of a suspicious or dangerous nature. As part of security awareness, it is also important to establish a reporting structure in advance so employees know whom to tell and how to describe what is being reported.

Key Prevention Capabilities

- All transportation employees contribute to security and prevention.
- Establishing security awareness of all employees can support prevention.
- Because of their constant presence on agency premises, employees are uniquely positioned to identify issues, problems, and deviations from the usual.
- Security and safety are centrally led activities.
- Focus security awareness on supporting business needs and processes such as critical infrastructure, DOT vehicles and maintenance facilities, and transportation management centers.
Establishing a reporting structure in advance—whom to tell and how to describe something suspicious—is critical to a security awareness program.

**Prevention Resources**

This report outlines techniques to integrate all-hazards security awareness concepts and reminders into routine state DOT operations, maintenance, and training.

This guidebook provides an overview of the mission and functions of transportation management centers, emergency operations centers, and fusion centers. The guidebook focuses on the types of information these centers produce and manage and the ways that the sharing of such information among the centers can be beneficial to both the day-to-day and emergency operations of all the centers.

This guide is designed to provide transportation managers and employees with an introductory-level reference document to enhance their working knowledge of security concepts, guidelines, definitions, and standards.

The intent of this report is to recommend policies and actions to reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and sociopolitical damage.

*Information Sharing and Analysis Centers (ISACS)*
ISACs are trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government. ISACs take an all-hazards approach and provide services that include alert and information sharing, risk mitigation, and incident response. Transportation-specific ISACs include:

- **Surface Transportation ISAC**
  https://www.surfacetransportationisac.org/
  The ST-ISAC was formed at the request of the U.S. Department of Transportation. The ST-ISAC provides a secure cyber and physical security capability for owners, operators, and users of critical infrastructure. Security and threat information is collected from worldwide resources, then analyzed
and distributed to members to help protect their vital systems from attack. The ST-ISAC also provides a vehicle for the anonymous or attributable sharing of incident, threat, and vulnerability data among the members.

• **Public Transportation Information Sharing and Analysis Center**  
The PT-ISAC provides an electronic, trusted ability for the membership to exchange and share information on all threats, physical and cyber, in order to defend public transportation systems and critical infrastructure. This includes analytical support to the government and other ISACs regarding technical sector details and in mutual information sharing and assistance during actual or potential sector disruptions, whether caused by intentional or natural events.

• **Over-the-Road Bus Information Sharing and Analysis Center (OTRB ISAC)**  
  [https://www.surfacetransportationisac.org/](https://www.surfacetransportationisac.org/)  
The OTRB ISAC provides cyber and physical security warning and incident reporting for the OTR transportation segment. Information and news are compiled and extracted from multiple sources by OTRB-ISAC analysts for the purpose of supporting ISAC member homeland security awareness. News alerts and reports are distributed to members.

• **Multistate-ISAC (MS-ISAC)**  
The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation, and incident response.

• **Supply Chain ISAC**  
  [https://secure.sc-investigate.net/sc-isac/isachome.aspx](https://secure.sc-investigate.net/sc-isac/isachome.aspx)  
The Supply Chain ISAC offers the most comprehensive forum for collaboration on critical security threats, incidents, and vulnerabilities to the global supply chain. Its mission is to facilitate communication among supply chain-dependent industry stakeholders; foster a partnership between the private and public sectors to share critical information, and collect, analyze and disseminate actionable intelligence to help secure the global supply chain; provide an international perspective through private sector subject matter experts; and help protect critical U.S. infrastructure.

• **First Observer™**  
  [https://www.tsa.gov/for-industry/firstobserver](https://www.tsa.gov/for-industry/firstobserver)  
The First Observer™ Program is a voluntary program that provides transportation professionals with training on effectively observing, assessing and reporting suspicious individuals, vehicles, packages, and objects.
Establishing and maintaining an all-hazards infrastructure protection program designed to (1) safeguard personnel; (2) prevent unauthorized access; and (3) safeguard infrastructure, facilities, equipment, installations, materiel, and data.

Infrastructure protection is integral to an all-hazards approach to preparedness. Protection includes the identification of critical assets and managing risks, assessment of their vulnerability/potential consequences, and development and deployment of suitable countermeasures and adaptation strategies.

**Figure 11. National Infrastructure Protection Plan**

*Source: DHS (2006)*

**Key Protection Capabilities**

- Includes risk management and risk assessment, plans and strategies, and countermeasures and adaptations.
- Understand the sensitivity of system assets, infrastructure, and services to different types of events.
- Understand interdependency of critical infrastructure.
- Integrate asset protection with broader transportation planning efforts, such as identification of long-term transportation capacity needs.
- Consider countermeasures to address possible vulnerabilities such as access control and system hardening for both physical and cyber security.
Figure 12. Layers of Security.

Many, if not all, DOTs have conducted vulnerability assessments of their critical assets. Figure 13 provides an overview of the factors and attributes to consider for assessments as recommended by the Blue Ribbon Panel on Bridges and Tunnels.
Figure 13. Components in Risk Assessment for a Facility

Protection Resources

This guide is designed to provide transportation managers and employees with an introductory-level reference document to enhance their working knowledge of security concepts, guidelines, definitions, and standards.

The guide provides code-ready language containing general design guidance and a simplified design procedure for blast-resistant reinforced concrete bridge columns. The report also examines the results of experimental blast tests and analytical research on reinforced concrete bridge columns designed to investigate the effectiveness of a variety of different design techniques.

This report recommends policies and actions to reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and sociopolitical damage.
This guide is designed as a planning tool for top-down estimation of both capital and operating budget implications of measures intended to reduce risks to locally acceptable levels. CAPTA supports mainstreaming an integrated, high-level, all-hazards, National Incident Management System (NIMS)—a responsive, multimodal, consequence-driven risk-management process into transportation agency programs and activities.

The FHWA developed this guide to help transportation agencies become familiar with the CAPTA methodology and learn how to use CAPTool in capital budget and decision making.
Mitigation

Preventing hazards from developing into disasters, or reducing the effects or mitigating the consequences of ongoing events. It focuses on long-term measures for reducing or eliminating risk and can occur prior to a disaster as an element of preparedness, or as a part of recovery when rebuilding following a disaster.

DOTs need to focus on long-term measures for reducing or eliminating risk in transportation physical and cyber infrastructure. This responsibility extends to both transportation and non-transportation infrastructure because of the interdependencies of state systems and functions. For this reason, DOT mitigation efforts should be integrated into overall state, local, and regional hazard mitigation assessment and mitigation plans. Mitigation can occur prior to a disaster as an element of preparedness, or as a part of recovery when rebuilding following a disaster. Mitigation can be structural, as in retrofitting bridges to better withstand earthquakes, or non-structural, as in establishing processes and procedures to minimize the consequences of a cybersecurity incident.

Key Mitigation Capabilities

- Conduct vulnerability assessments to identify known and unknown risks, present and future.
- Identify key dependencies and interdependencies, including mapping potential cascading effects from potential infrastructure disruptions.
- Monitor likely problem areas and explore mitigation/resiliency strategies to minimize impact. Examine activities to reduce asset loss or human consequences (such as injuries or fatalities).
- Collaborate with regional partners and stakeholders.
- Consider applicable standards and best practices for mitigation plans and for incorporating resilience into asset and system design.
- Identify mitigation approaches such as seismic retrofitting, elevation changes, and flood proofing. Determine whether adaptations such as environmental buffers can be incorporated into the infrastructure design to mitigate the effects of natural disasters.

![Figure 14. Steps in Vulnerability Assessment](https://example.com/image.png)

Figure 15. FWHA Framework for Vulnerability Assessment

Source: Assessing Vulnerability and Risk of Climate Change Effects on Transportation Infrastructure (2014)
**Mitigation Resources**

*Case Study in Bridge and Tunnel Risk Assessment* (2003), Appendix C: Recommendations for Bridge and Tunnel Security


This appendix to the Blue Ribbon Panel Report describes the risk assessment method used to help determine how to allocate resources for mitigating the adverse effects of terrorist acts on critical transportation facilities and the occupants of those facilities.


http://www.fhwa.dot.gov/environment/climate_change/adaptation/ongoing_and_current_research/vulnerability_assessment_pilots/conceptual_model62410.cfm

FHWA's document outlines a conceptual risk assessment model piloted in state DOTs or MPOs that is being developed into a final version for all transportation agencies.


http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2ndEdition.pdf

The guide includes a five-step process for conducting a threat and hazard identification and risk assessment (THIRA).


http://www.fema.gov/media-library/assets/documents/34374

This FEMA factsheet provides summary information for the THIRA.


http://highwaytransport.transportation.org/Documents/NCHRP_B.pdf

This AASHTO guide provides state DOTs with information about how to conduct a vulnerability assessment. Information about assessment methods of state and federal agencies is included along with illustrative examples.

See also the [Protection Resources](#) on pages 31–32.
Providing transportation (including infrastructure access and accessible transportation services) for (1) response priority objectives, including the evacuation of people and animals; and (2) the delivery of vital response personnel, equipment, and services to the affected areas.

Transportation plays a critical role in an emergency situation. State DOTs must be prepared to effectively respond to and quickly recover from many types of events. Other state agencies rely on DOTs to provide support during a major disaster. During an event, the success of any response depends largely on the strength of relationships among local law enforcement, emergency response personnel, and DOT local staff.

Key Response Capabilities

• Develop skilled DOT response teams equipped to handle an array of events such as tunnel emergencies or bridge failures.
• Establish protocols for use of traffic cameras for critical infrastructure surveillance during emergency events.
• Develop memoranda of understanding (MOU) with other local and state agencies. Establish and maintain mutual aid agreements with fire departments, emergency medical services, and emergency management services.
• Ensure that the agency formalizes its approach to evacuation management, including plans, policies, and procedures for evacuations with or without notice.
• Document expenses consistent with reimbursement practices of FEMA or others.

“Our focus is simple. We will provide the road to safety, we will clear the road to recovery, and we will maintain the road home.”

—Former DOT Executive Director
### Figure 16. Actions and Activities to Be Included in an Ideal Emergency Operations Plan


<table>
<thead>
<tr>
<th>Step</th>
<th>Phase</th>
<th>Action Item</th>
<th>Supporting Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan</td>
<td></td>
<td>Form a collaborative planning team.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conduct research and analyze the data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determine goals and objectives.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop and analyze courses of action and identify resources.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Write the plan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approve and implement the plan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exercise the plan and evaluate its effectiveness.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review, revise, and maintain the plan.</td>
<td></td>
</tr>
<tr>
<td>Prepare</td>
<td></td>
<td>Develop approaches to implement state transportation agency roles and responsibilities during emergencies, as specified in the state EOP (SEOP), supporting annexes, and referenced materials.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establish protocols to communicate with employees and the general public.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop plans and procedures to manage traffic under emergency conditions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop mobilization plans to ensure readiness to deploy state transportation agency personnel and resources.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure cost tracking and accountability.</td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td>Initiate emergency response.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Address emergency needs and requests for support.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manage evacuation/shelter-in-place/quarantine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implement emergency response actions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continue response.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conclude response.</td>
<td></td>
</tr>
</tbody>
</table>
Response Resources

National Response Framework (2013)
https://www.fema.gov/national-response-framework
The National Response Framework provides context for how the whole community works together and how response efforts relate to other parts of national preparedness. It addresses the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. Emergency Support Functions (ESFs) are established under the National Response Framework.

Information Sheet ESF #1 Transportation
https://www.fema.gov/media-library/assets/documents/32171
Emergency Support Function (ESF) #1—Transportation provides support by assisting local, state, tribal, territorial, insular area, and federal governmental entities, voluntary organizations, nongovernmental organizations, and the private sector in the management of transportation systems and infrastructure during domestic threats or in response to actual or potential incidents.

This Guide provides an overview of high-level requirements for emergency response planning based on national policies, an agency self-assessment, and a resource guide with organization staffing guidance, decision-making sequences, and resource lists.

Role of Transportation Management Centers in Emergency Operations Guidebook (2012)
This FHWA guidebook covers ways to increase communication and collaboration between transportation management centers and emergency response agencies.

Information-Sharing Guidebook for Transportation Management Centers, Emergency Operations Centers, and Fusion Centers (2010)
This guidebook provides an overview of the mission and functions of transportation management centers, emergency operations centers, and fusion centers. It focuses on the types of information these centers produce and manage and how the sharing of such information among the centers can be beneficial to both day-to-day and emergency operations of all the centers.
Recovery

Efficiently restoring infrastructure systems and services to support a viable, sustainable community; and improving resilience to and protection from future hazards.

DOTs need to quickly and efficiently implement recovery after incidents and events. Planning for recovery and having a recovery organization with clear authority and responsibilities identified prior to the event can expedite recovery. Quick response to an event that damages infrastructure can mitigate the losses and shorten the time necessary to recover. Short-term recovery decisions can have long-term implications. For example, bridge closures, locations selected for debris sites, and decisions about infrastructure restoration can limit longer-term options.

Key Recovery Capabilities

• Develop a COOP to ensure rapid recovery from incidents or events. As part of COOP, an annex on reconstruction can be used to include information on which infrastructure assets might need to be replaced or relocated.
• Establish trained, skilled teams for rapid clean up, repair, and inspection after an incident or event.
• Conduct damage assessments, debris removal, hazardous materials disposal, and repair of roads and other facilities to restore essential services to the affected area.
• Develop an approach to infrastructure repair and/or replacement and decontamination in advance. Implement improved materials and construction methods to prevent similar damage from occurring again.
• Identify lessons learned through After-Action Review (AAR) and incorporate recommendations into existing plans and procedures.
### Recovery Phases

**Pre-Disaster Preparedness**
- Ongoing
  - Plan for recovery
  - Assess risks
  - Organize resources, build partnerships

**Short-Term Recovery**
- Days
  - Support mass care, sheltering, emergency services, and temporary infrastructure for business reopenings
  - Clear primary transportation routes (debris removal)

**Intermediate Recovery**
- Weeks/Months
  - Repair/restore urgently needed infrastructure
  - Support interim housing, business reestablishment, and public healthcare

**Long-Term Recovery**
- Months/Years
  - Rebuild infrastructure to meet future needs
  - Implement mitigation activities and build resilience

*Figure 17. Recovery Phases*

*Source: Adapted from the National Disaster Recovery Framework, FEMA/DHS (2011)*
### Figure 18. COOP Time-Phased Implementation

**Source:** Continuity of Operations Planning Guidelines for Transportation Agencies (2005)

#### Recovery Resources


http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_753.pdf

This guide was designed to help transportation owners and operators in their efforts to plan for recovery prior to the occurrence of an event that impacts transportation systems. The guide is intended to provide a single resource for understanding the principles and processes to be used in pre-event recovery planning for transportation infrastructure and includes tools and resources to assist in both pre-planning for recovery and implementing recovery after an event.
The guidelines were designed to assist transportation agencies in operations plans, policies, and procedures consistent with the National Incident Management System. Downloadable worksheets, a template for a COOP plan, brochures to explain the COOP planning process to staff, a customizable PowerPoint for executive leadership, and 300-plus resources organized in an electronic library are included.

National Disaster Recovery Framework (2011)
http://www.fema.gov/media-library/assets/documents/24647
The National Disaster Recovery Framework is a guide that enables effective recovery support to disaster-impacted states, tribes, territorial, and local jurisdictions. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. The framework introduces six recovery support functions that provide a structure to facilitate problem solving, improve access to resources, and foster coordination among state and federal agencies, nongovernmental partners, and stakeholders.

http://transweb.sjsu.edu/project/1080.html
Homeland Security Presidential Directive 20 (HSPD-20) requires all local, state, tribal, and territorial government agencies, and private sector owners of critical infrastructure and key resources (CI/KR) to create a Continuity of Operations/Continuity of Government Plan (COOP/COG). This report covers the research conducted to determine how to integrate COOP/COG into the overall NIMS approach to emergency management, including a connection between the emergency operations center (EOC) and the COOP/COG activity. The first section is a presentation of the research and its findings and analysis. The second section provides training for the EOC staff of a state-level transportation agency, using a hybrid model of FEMA’s ICS and ESF approaches, including a complete set of EOC position checklists, and other training support material. The third section provides training for the COOP/COG Branch staff of a state-level transportation agency, including a set of personnel position descriptions for the COOP/COG Branch members.
Establishing and maintaining a program designed to (1) safeguard transportation control systems, enterprise data systems, and communications systems; (2) prevent unauthorized access; (3) safeguard equipment, installations, materiel, and data; and (4) minimize the consequences of an intentional or unintentional cyber incident.

There is an increased probability that cyber incidents (intentional and unintentional) will occur more frequently at DOTs due to increasing convergence and dependence on digital components and systems. Although there are parallels to physical security, significant differences in terminology, risk and vulnerability, countermeasures, personnel, and training exist in cybersecurity. Controls system cybersecurity is not the same as IT cybersecurity. Implementing cybersecurity for transportation control systems requires having a good understanding of security and the controls systems and the operational environments.

**Key Cybersecurity Capabilities**
- Integrate cybersecurity decision making into business processes and investments.
- Evaluate and manage agency-specific cyber risks.
- Implement industry standards and best practices.
- Facilitate discussion and interaction between information technology, engineering, and operational groups to ensure that all systems are adequately addressed. Coordinate cybersecurity and cyber incident response planning across the enterprise.

![Cybersecurity Risk-Based Framework](source: NIST Cybersecurity Framework)
Figure 20. NIST Framework Implementation Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Inputs</th>
<th>Activities</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk management strategy Organizational objectives and priorities Threat information</td>
<td>Determine where to apply framework to evaluate and guide cybersecurity capabilities</td>
<td>Scope of framework in organization</td>
</tr>
<tr>
<td>2</td>
<td>Risk management strategy Framework scope</td>
<td>Identify in-scope systems and assets Identify standards, guidelines, and tools</td>
<td>Systems and assets Cybersecurity requirements and standards Evaluation approach</td>
</tr>
<tr>
<td>3</td>
<td>Evaluation approach Systems and assets Requirements and standards</td>
<td>Identify current cybersecurity and risk management state</td>
<td>Current profile</td>
</tr>
<tr>
<td>4</td>
<td>Risk management strategy Evaluation approach Systems and assets Requirements and standards</td>
<td>Perform risk assessment</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>5</td>
<td>Current profile Organizational objectives Risk management strategy Risk assessment reports</td>
<td>Identify goals to mitigate risk consistent with organizational goals and critical infrastructure objectives</td>
<td>Target profile</td>
</tr>
<tr>
<td>6</td>
<td>Current profile Target profile Organizational objectives Organizational constraints Risk management strategy Risk assessment</td>
<td>Analyze gaps between current and target profile Evaluate consequences from gaps Prioritize actions (cost–benefit analysis, consequences) Create action plan</td>
<td>Prioritized gaps Prioritized implementation plan</td>
</tr>
<tr>
<td>7</td>
<td>Prioritized implementation plan</td>
<td>Implement actions by priority Track progress against plan Monitor/evaluate progress against risks, metrics, and performance indicators</td>
<td>Project tracking data New security measures implemented</td>
</tr>
</tbody>
</table>

**Cybersecurity Resources**

*Effective Practices for the Protection of Transportation Infrastructure from Cyber Incidents* (anticipated in 2015; weblink not yet available)

This NCHRP/TCRP guide provides an overview of the nature of transportation system cyber events and their operational and safety impacts and includes effective practices that can be used to protect transportation systems from cyber events and to mitigate damage should an incident or breach occur.
This NIST guide advises on how to reduce the vulnerability of computer-controlled industrial control systems to malicious attacks, equipment failures, errors, inadequate malware protection, and other software-related threats. The guide includes sections on ICS threats and vulnerabilities, risk management, recommended practices, security architectures, and security capabilities and tools for ICS.

APTA Standards Development Program Recommended Practice: Securing Control and Communications Systems in Transit Environments

- **Part I: Elements, Organization, and Risk Assessment/Management (2010)**
  This recommended practice addresses the importance of control and communications security to a transit agency; provides a survey of the various systems that constitute typical transit control and communication systems; identifies the steps that an agency would follow to set up a successful program; and establishes the stages of conducting a risk assessment.

- **Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones (2013)**
  This recommended practice covers how to define security architecture for control and communications systems and presents “defense-in-depth” as a recommended approach for securing rail communications and control systems. It defines security zone classifications, and defines a minimum set of security controls for the most critical zones: the safety-critical security zone (SCSZ) and the fire, life-safety security zone (FLSZ).

  This white paper will cover recommended practices for operationally critical security zones, security zones onboard the train consist, and attack modeling for transit.

NIST Cybersecurity Framework
http://www.nist.gov/cyberframework/
The NIST framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure.
Training and Exercises

Preparing DOT employees for their roles; understanding and improving plans put in place; and providing an opportunity to test plans and validate the effectiveness of training.

DOTs need to understand the importance of training and exercises to maintain plans and practice their use. Generally, individuals are trained in their tasks and then teams are brought together to train on integrated tasks. Training may be classroom, at the DOT or another location; online through the Federal Emergency Management Agency (FEMA) or other organization; or may occur on the job to build depth in capabilities, such as at an EOC. An effective exercise program is an essential component of preparedness as it validates plans, tests operational capabilities, maintains leadership effectiveness, and examines ways the whole emergency management community is utilized.

Key Training and Exercise Capabilities

- Ensure that DOT employees receive training to prepare them for their roles and that they are able to practice what they have been taught to increase the effectiveness of the training.
- Incorporate security awareness into existing training, such as in new or existing employee training, including position-specific training where relevant. For example, Texas DOT incorporates security awareness information into bridge inspector training, highlighting the need to be vigilant and to pass along information.
- Keep training, drills, and contact lists up to date.
- Identify lessons learned through after action report and incorporate recommendations into existing plans and procedures.

The types of training in a DOT may include:

- Security awareness
- Infrastructure protection, e.g. bridge security and protection
- National Incident Management System (NIMS)
- Traffic Incident Management (TIM)
- Emergency response and disaster recovery exercises, e.g. Homeland Security Exercise and Evaluation Program (HSEEP)
- Position-specific training

**Figure 21. Training Approach**

Training and Exercises Resources

This report provides guidelines, resources, and templates for developing a progressive exercise program, compliant with DHS and ODP requirements.

FEMA Emergency Management Institute (EMI)
http://training.fema.gov/emi.aspx
EMI provides training to federal, state, local, tribal, volunteer, public, and private sector officials to strengthen emergency management core competencies for professional, career-long training. It directly supports the implementation of the National Incident Management System (NIMS), the National Infrastructure Protection Plan (NIPP), National Response Framework (NRF), the National Disaster Recovery Framework (NDRF), and the National Preparedness Goal (NPG).

http://transweb.sjsu.edu/project/1103.html
The U.S. Department of Homeland Security (DHS) has provided extensive general guidance on developing training and exercise programs for public entities but little had been done to focus that material on the transportation sector specifically. Transportation sector emergency managers have noted that there should be specific guidance for developing exercises that are focused on the operational work of their agencies, in addition to the logistics section functions that are usually the focus of transportation sector entities in multiagency, multijurisdictional exercises. The first section of this report provides information on federal training and exercise requirements for transportation sector entities. It summarizes the changes to emergency management programs and requirements that grew out of the Presidential Policy Directive 8 (PPD-8) issuance in early 2011 and the challenges of adult training. The second section is a Homeland Security Exercise and Evaluation Program (HSEEP)-compliant practical handbook using the project management approach that guides transportation sector staff in the creation, development, implementation, and wrap-up of federally mandated exercises. It includes scenarios and implementation guidance based on the actual experiences and work of the transportation sector.

http://www.trb.org/PlanningForecasting/Blurbs/172182.aspx
Identifies interactive emergency training tools and sources that may be applied by maintenance and operations field personnel of state departments of transportation and public works agencies. The report also identifies potential obstacles to their implementation and develops a toolkit of relevant training and exercise information.
http://www.trb.org/Main/Blurbs/171543.aspx
Outlines techniques to integrate all-hazards security awareness concepts and reminders into routine state department of transportation (DOT) operations, maintenance, and training.

NCHRP 20-59(30): Incident Command System (ICS) Training for Field Level Transportation Supervisors and Staff
The objective of this research is to develop specialized Incident Command System (ICS) training for field level transportation supervisors and staff. The intended audience is state transportation agency field staff members, but the training would also be applicable to city and county transportation field staff members.

Transportation Emergency Response Application (TERA)
The National Guard Bureau and the TRB Cooperative Research Programs have sponsored development of training simulation scenarios and no-license-fee systems on which to deploy them. Research is in progress to develop and improve additional scenarios specifically for DOTs, airports, and the transit industry, which would supplement discussion- and operations-based exercises as a means to simulate, train, and assess critical incident decision making reflecting real-world constraints. To do so, the scenarios and the system they are deployed on must be affordable, cost-effective, easy to set up and use, have readily available support, provide a measured assessment, and allow participants to exercise the resources and policies they currently use in response to emergencies. Emergency management professionals in the transportation, transit, rail, and airport domains may register to use TERA for free at www.tera.train-emst.com.
Appendix A: Selected References for Federal Frameworks and Initiatives


Overview of the National Planning Frameworks (2013)

National Planning Frameworks:
- National Prevention Framework
- National Protection Framework
- National Mitigation Framework
- National Response Framework
- National Disaster Recovery Framework


Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)


2013 National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience

NIPP Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects

NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach
Appendix B: Definitions

**Asset:** Any person, facility, material, information, or activity that has a positive value to the transportation systems sector. For a DOT, asset consist of people, information, and property for which the transportation system is responsible as legal owner, employer, or service provider. The asset value nature and magnitude of those values may differ according to asset owner, operator, and user. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, and information) or intangible (e.g., processes or an agency’s information and reputation).

**Critical Assets:** A subcategory of assets essential to the minimum operations of the organization, and to the health and safety of the general public, loss of which has the greatest consequences for people and the ability of the system to sustain service. Such an asset supports national security, national economic security, and/or crucial public health and safety activities (CIAO). A state DOT’s critical assets may include, but are not limited to, bridges, major tunnels, operations and management centers, vehicles, and key intermodal facilities. Transportation infrastructure facilitates the movement of people, services, and cargo, and some elements are critical to the maintenance of public health, economic vitality, telecommunications, electricity, and other essential services. For example, the temporary debilitation of a bridge or tunnel could result in regional shutdowns, diversions, or costly repairs with potentially severe results.

**Asset Protection:** Security program designed to protect personnel, facilities, and equipment, in all locations and situations; accomplished through planned and integrated application of counter-terrorism, physical security, operations security, and personal protective services; and supported by intelligence, counter-intelligence, and other security.

**Catastrophic Incident:** Any natural or man-made incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in sustained regional or national impacts over a prolonged time period; almost immediately exceeds resources normally available to state, territorial, local, tribal, and private-sector authorities in the affected area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.

**Countermeasure:** An action intended to induce institutional, process, and physical changes that reduce risks to systems and assets. The countermeasure may address a vulnerability, threat, consequence, or overall system performance.

**Continuity of Operations (COOP):** An effort within individual organizations to ensure that primary mission essential functions continue to be performed during a wide range of emergencies. A comprehensive COOP plan provides a framework that establishes operating procedures to sustain essential functions when
normal procedures are not possible and provides a guide for restoring normal agency operations and building functions.

**Disaster Mitigation:** Measures, procedures, and strategies designed to reduce either the likelihood or consequences of a disaster.

**Disaster Recovery:** Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

**Disaster Recovery Center (DRC):** Place established in the area of a presidentially declared major disaster, as soon as practicable, to provide victims the opportunity to apply in person for assistance and/or obtain information relating to that assistance.

**Disaster/Emergency Management Program:** A program that implements the mission, vision, and strategic goals and objectives as well as the management framework of the program and organization.

**Emergency:** Any incident, whether natural or man-made, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the president, federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.


**Emergency Management Assistance Compact (EMAC):** A national, interstate mutual-aid agreement that enables states to share resources during times of disaster. EMAC has grown to become the nation’s system for providing mutual aid through operational procedures and protocols that have been validated through experience. EMAC is administered by NEMA, the National Emergency Management Association, headquartered in Lexington, KY. EMAC acts as a complement to the federal disaster response system, providing timely and cost-effective relief to states requesting assistance from assisting member states. [Adapted from FEMA-EMAC, 2007. Available at [http://www.gao.gov/products/GAO-07-854](http://www.gao.gov/products/GAO-07-854).] It is also available for local mutual-aid assistance in states that have passed enabling legislation.

**Emergency Management Response Personnel:** Includes federal, state, territorial, tribal, substate regional, and local governments; private sector organizations; critical infrastructure owners and operators; non-governmental organizations; and all other organizations and individuals who assume an emergency management role. Also known as Emergency Responder.

**Emergency Operations Center (EOC):** Special policy and incident management area, activated under certain conditions and staffed by representatives from the transportation system, including top management, to serve as an information coordination point during special events or emergencies and to authorize decisions
that either require or affect the legal authority of the system. The main functions of an EOC include providing direction, coordination, and support to emergency operations; carrying out disaster management functions at a strategic level in an emergency; and ensuring the continuity of operation of an agency, political subdivision, or other organization. The EOC also collects, gathers, and analyzes data; makes decisions that protect life and property; maintains continuity of the organization; and disseminates those decisions to all concerned agencies and individuals. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., federal, state, regional, county, city, tribal), or some combination thereof.

**Emergency Operations Plan (EOP):** An ongoing plan maintained by various jurisdictional levels for responding to a wide variety of potential hazards. Document that describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.

**Emergency Plan:** A brief, clear, and concise description of the overall emergency organization, designation of responsibilities, and descriptions of the procedures, including notifications, involved in coping with any or all aspects of a credible potential emergency.

**Emergency Preparedness:** 1. A uniform basis for operating policies and procedures for mobilizing the transportation system and other public safety resources to assure rapid, controlled, and predictable responses to various types of transportation and community emergencies. 2. The training of personnel; acquisition and maintenance of resources; and exercising of the plans, procedures, personnel, and resources essential for emergency response.

**Emergency Response:** The planned and actual response by multiple agencies to incidents that can include acts of terrorism, wildland and urban fires, floods, hazardous material spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, and public health and medical emergencies. The phases of ER are plan, prepare, respond, and recover (National Response Framework, 2008; available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf).

**Emergency Transportation Operations (ETO):** A coordinated, performance-oriented, all-hazards approach to support the development of a formal program for the improved management of traffic incidents, natural disasters, security events, and other emergencies on the highway system. Focuses on an enhanced role for state DOTs as participants with the public safety community in an interagency process. (Adapted from NCHRP Report 525, Volume 6, 2005.)

**Emergency Support Function (ESF):** In the Federal Response Plan (FRP), a functional area of response activity established to facilitate the delivery of federal assistance required during the immediate response phase of a disaster to save lives, protect property and public health, and maintain public safety. ESFs represent those types of federal assistance that the state will most likely need because of the impact of a catastrophic or significant disaster on its own resources and response capabilities, or because of the specialized or unique nature of the assistance required. ESF missions are designed to supplement state and local response efforts.
**Exercise:** An instrument to train for, assess, practice, and improve performance in prevention, protection, response, and recovery capabilities in a risk-free environment. Exercises can be used for: testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement.

**First Responder:** Those individuals who are responsible in the early stages of an incident for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 11), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) who provide immediate support services during prevention, response, and recovery operations (HSPD-8).

**Full-Scale Exercise (FSE):** A multiagency, multijurisdictional activity involving actual deployment of resources in a coordinated response as if a real incident had occurred. An FSE tests many components of one or more capabilities within emergency response and recovery, and is typically used to assess plans and procedures and coordinated response under crisis conditions. Characteristics of an FSE include mobilized units, personnel, and equipment; a stressful, realistic environment; and scripted exercise scenarios.

**Fusion Center (FC):** A collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel; training; technical assistance; exercise support; security clearances; and connectivity to federal systems, technology, and grant funding. FCs are referred to differently in the various states. For more information, see FHWA’s Information-Sharing Guidebook for Transportation Management Centers, Emergency Operations Centers, and Fusion Centers (2010), available at [http://www.ops.fhwa.dot.gov/publications/fhwahop09003/](http://www.ops.fhwa.dot.gov/publications/fhwahop09003/).

**General Staff:** A group of incident management personnel organized according to function and reporting to the incident commander. The general staff normally consists of the operations section chief, planning section chief, logistics section chief, and finance/administration section chief. An intelligence/investigations chief may be established, if required, to meet incident management needs.

**Hazard:** An event or physical condition that has the potential to cause fatalities, injuries, property damage, infrastructure damage, agricultural loss, damage to the environment, interruption of business, or other types of harm or loss.

**Hazard Mitigation:** Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event.

**Hazardous Material (HazMat):** Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people’s health, safety, and/or property. These substances and materials
include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

**Homeland Security:** The federal government’s efforts, in coordination with state and local governments and the private sector, to develop, coordinate, fund, and implement the programs and policies necessary to detect, prepare for, prevent, protect against, respond to, and recover from terrorist or other attacks within the U.S.

**Homeland Security Exercise Evaluation Program (HSEEP):** A capabilities- and performance-based exercise program that provides standardized policy, doctrine, and terminology for the design, development, conduct, and evaluation of homeland security exercises. HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.

**Incident:** An occurrence that has been assessed as having an adverse effect on the performance of critical infrastructure. The occurrence or event, natural or human-caused, requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response. Traffic incidents are considered as included, even if minor.

**Incident Action Plan:** An oral or written plan containing general objectives reflecting the overall strategy for managing an incident.

**Incident Command:** Responsible for overall management of the incident and consists of the incident commander, either single or unified command, and any assigned supporting staff.

**Incident Command Post (ICP):** The field location at which the primary tactical-level, on-scene incident command functions are performed. The ICP may be collocated with the incident base or other incident facilities and is normally identified by a green rotating or flashing light.

**Incident Commander (IC):** The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and release of resources. The IC has overall authority and responsibility for conducting incident operations and for the management of the incident site.

**Incident Command System (ICS):** A standardized organizational structure used to command, control, and coordinate the use of resources and personnel assigned to the scene of an emergency. The concepts and principles for ICS include common terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.

**Incident Management:** The broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all levels of government, utilizing both governmental and nongovernmental resources to plan for, respond to, and recover from an incident, regardless of cause, size, or complexity.

**Incident of National Significance:** Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high-impact event that requires a coordinated and effective response by an appropriate combination
of federal, state, local, tribal, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and to provide the basis for long-term community and economic recovery.

**Infrastructure Protection:** Strategies and actions to strengthen critical assets, improve security capabilities, and provide increased resilience of transportation systems, networks, and assets.

**Interdependency:** The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

**Intermediate Recovery:** Recovery phase that involves returning critical infrastructure and essential services back to a functional if not predisaster state. Such activities are often characterized by temporary actions that provide a bridge to permanent measures.

**Intermodal:** Those issues or activities that involve or affect more than one mode of transportation including transportation connections, choices, cooperation, and coordination of various modes. Also known as “multi-modal.”

**Interoperability:** Allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions via voice, data, or video-on-demand, in real-time, when needed, and when authorized.

**Jurisdiction:** A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographic (e.g., city, county, tribal, state, or federal boundary lines) or functional (e.g., law enforcement, public health).

**Jurisdictional Agency:** The agency having jurisdiction and responsibility for a specific geographical area or a mandated function.

**Long-Term Recovery:** Process of recovery that follows a disaster event and may continue for months and years. An example is the complete redevelopment and revitalization of the damaged area, which could mean returning to conditions set in a long-term recovery plan.

**Major Disaster:** As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of cause, any fire, flood, or explosion, in any part of the U. S., that in the determination of the president causes damage of sufficient severity and magnitude to warrant major disaster assistance under this act to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby. The 2010 Planning for Emergency Response treats a catastrophic event as a more severe event than a major disaster. For example, Hurricane Rita might be considered as a major disaster while Katrina was, and continues to be, catastrophic.

**Memoranda of Understanding (MOU):** Written or oral mutual-aid agreements that serve as the basis of mutual acknowledgement of the resources that each organization will provide during response and recovery efforts.
Mitigation: Action taken to prevent hazards from developing into disasters, or to reduce the effects or alleviate the consequences of disasters when they occur. Mitigation activities provide a critical foundation in the effort to reduce the loss of life and property from natural and/or man-made disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer transportation systems and communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage by focusing on long-term measures for reducing or eliminating risk. Mitigation actions can occur prior to a disaster as an element of preparedness, or as a part of recovery when rebuilding following a disaster.

Multiagency Coordination (MAC) Group: Typically, administrators/executives, or their appointed representatives who are authorized to commit agency resources and funds, are brought together and form MAC Groups. MAC Groups may also be known as multiagency committees, emergency management committees, or as otherwise defined by the system.

Multiagency Coordination Entity: Functions within a broader multiagency coordination system. It may establish the priorities among incidents and associated resource allocations, deconflict agency policies, and provide strategic guidance and direction to support incident management activities.

Multiagency Coordination System (MACS): Provides the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. Elements include facilities, equipment, personnel, procedures, and communications. Two of the most commonly used elements are EOCs and MAC groups. These systems assist agencies and organizations responding to an incident.

Multijurisdictional Incident: An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under unified command.

Mutual Aid Agreements and/or Assistance Agreements: Written or oral agreements between and among agencies/organizations and/or jurisdictions that provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

National Incident Management System (NIMS): A set of principles that provides a systematic, proactive approach guiding government agencies at all levels; nongovernmental organizations; and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.

Natural Hazard: Naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property (FEMA 386-2, Mitigation Planning How-To Guide #2: Understanding Your Risks). The risks of natural hazards may be increased or decreased as a result of human activity; however, they are not inherently human-induced.

National Response Framework (NRF): Government resources alone cannot meet all the needs of those affected by terrorist attacks, natural disasters and other catastrophic events. When disaster strikes, people through-
out the community and our nation pitch in to help the response effort. The second edition of the National Response Framework (NRF), updated in 2013, provides context for how the whole community works together and how response efforts relate to other parts of national preparedness. It is one of the five documents in a suite of National Planning Frameworks. Each Framework covers one preparedness mission area: Prevention, Protection, Mitigation, Response or Recovery. The new NRF incorporates a focus on whole community and core capabilities. For example, the Framework now describes the important roles of individuals, families and households in response activities.

**National Special Security Events (NSSE):** Events of national significance which by virtue of their political, economic, social, or religious significance may be targets of terrorism or other criminal activity. Events include presidential inaugurations, major international summits held in the U.S., major sporting events, and presidential nominating conventions.

**Nongovernmental Organization (NGO):** An entity with an association that is based on interests of its members, individuals, or institutions. It is not created by a government but it may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross.

**Participating Agency:** Any fire, law enforcement, medical, governmental, or humanitarian agency that participates in any portion of a transportation system’s emergency response.

**Preparedness:** A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination for emergency management and incident response before a potential incident. Organizations involved in preparedness range from groups of individuals to small committees to large standing organizations that represent a wide variety of committees, planning groups, and other organizations (e.g., citizen corps, local emergency planning committees (LEPCs), critical infrastructure sector coordinating councils).

**Prevention:** Actions to avoid an incident or to intervene to stop an incident from occurring. Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.

**Protection:** Establish and maintain an all-hazards infrastructure protection program designed to (1) safeguard personnel; (2) prevent unauthorized access; and (3) safeguard infrastructure, facilities, equipment, installations, materiel, and data.

**Recovery:** Capabilities necessary to efficiently restore infrastructure systems and services to support a viable, sustainable community and improve resilience to and protection from future hazards. May include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of operations and services; long-term measures for social, environmental, and economic restoration; evaluation of the incident to identify lessons; post-incident reporting; and development of initiatives to mitigate the effects of future incidents.
Recovery Plan: A plan developed by a state, local, or tribal jurisdiction with assistance from responding federal agencies to restore the affected systems or area.

Regional Planning Organization (RPO): An organization that performs planning for multijurisdictional areas. Metropolitan Planning Organizations, regional councils, economic development associations, and rural transportation associations are examples of RPOs.

Resilience: The ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events. (Committee on Increasing National Resilience to Hazards, Disasters and Committee on Science, Engineering, and Public Policy, The National Academies; Disaster Resilience: A National Imperative; The National Academies Press, 2012). Resilience 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.” Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, 2013).

Response: Immediate actions to save lives, protect property and the environment, and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery.

Restoration: Returning a physical structure, essential government or commercial services, or a societal condition back to its predisaster state through repairs, rebuilding, or reestablishment.

Risk Assessment: A comprehensive study of a transportation agency to identify components most vulnerable to criminal activity, including acts of terrorism and quasi-terrorism, and to assess the impact of such activity on passengers, employees, and the agency.

Risk Management: The process of selecting and implementing security countermeasures and mitigation strategies to achieve an acceptable level of risk. The process of measuring or assessing risk and then developing strategies to manage the risk. Involves a prioritization process through which risks with the greatest adverse consequences and greatest probability of occurring are handled first, and risks with lower probability of occurrence and lower loss are handled later if at all. Requires balancing risks with a high probability of occurrence but lower loss against risks with high loss but lower probability.

Risk Mitigation: The actions or decisions designed to reduce the financial and nonpecuniary risk from uncertain events.

Security: Freedom from harm resulting from intentional acts or circumstances. Reducing the risk to critical infrastructure by physical means or defensive 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 (Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, 2013).

Security Analysis: The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.
Security Awareness: The purpose of security awareness is to focus attention on security. It differs from security training, in that security awareness informs and draws attention to a security issue, but security training teaches the skills necessary to improve security.

Security Countermeasures: Actions that can be taken to avoid or mitigate security threats, the cornerstones of which are to detect, deter, deny, and defend. Some security countermeasures can actually impede emergency response; for example, the security need to have secure, qualified identifications of responders entering an incident scene might delay or even bar responders. This should be considered in the EOPs.

Security and Emergency Preparedness Plan: The formal plan that documents the transportation system’s security program and also addresses the elements of that program that affect emergency preparedness for events resulting from intentional acts.

Short-Term Recovery: Phase of recovery in which the scope of damages and needs are assessed, basic infrastructure is restored, and recovery organizations and resources are mobilized.

Standard Operating Guidelines: A set of instructions having the force of a directive, covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness.

Standard Operating Procedure (SOP): A complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner.

Tabletop Exercise (TTX): Intended to stimulate discussion of various issues regarding a hypothetical situation. TTXs can be used to assess plans, policies, and procedures or to assess types of systems needed to guide the prevention of, response to, or recovery from a defined incident. During a TTX, senior staff, elected or appointed officials, or other key personnel meet in an informal setting to discuss simulated situations. TTXs are typically aimed at facilitating understanding of concepts, identifying strengths and shortfalls, and/or achieving a change in attitude. Participants are encouraged to discuss issues in depth and develop decisions through slow-paced problem-solving rather than the rapid, spontaneous decision-making that occurs under actual or simulated emergency conditions. TTXs can be breakout (i.e., groups split into functional areas) or plenary (i.e., one large group).

Traffic Incident: Any nonrecurring event that reduces roadway capacity or abnormally increases demand. Such events include traffic crashes, disabled vehicles, spilled cargo, highway maintenance and reconstruction projects, and special nonemergency events (e.g., ball games, concerts, or any other event that significantly affects roadway operations) (Traffic Incident Management Handbook Update, FHWA, 2010).

Traffic Incident Management (TIM): A tool to achieve and maintain public safety, travel efficiency, and air quality standards by reducing the impacts of traffic incidents (I-95 Corridor Coalition Coordinated Incident Management, 2009; available at [http://www.i95coalition.org/wp-content/uploads/2015/03/toolkit_document_dvd1.pdf]). Can be considered a subset of emergency management.

Traffic Management Centers (TMCs): Operations centers responsible, usually 24/7, for monitoring and controlling traffic in designated sectors and for coordinating transportation agency response to emergencies.
Operated by local transportation agencies primarily in large urban areas. Many centers are now being collocated with other public safety, fire, and EMS responders. Some states are forming centers to manage traffic regionally. These regional centers are often referred to as traffic operations centers.

**Training:** An act, method, or process of instruction; to teach so as to make fit, qualified, or proficient.

**Unified Command (UC):** An incident command system application used when more than one agency has incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior persons from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single incident action plan.

**Unified Command System:** A unified team effort which allows all agencies with responsibility for the incident, either geographical or functional, to manage an incident by establishing a common set of incident objectives and strategies.

**Vulnerability:** A characteristic or flaw that renders an asset or system susceptible to destruction, incapacitation, or exploitation; characteristic of a critical infrastructure’s design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

**Vulnerability Assessment (VA):** Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or its product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation; a systematic evaluation process in which qualitative and/or quantitative techniques are applied to arrive at an effectiveness level for a safeguards-and-security system to protect specific targets from specific adversaries and their acts. In general, determining the vulnerability of a critical asset is the least difficult area of risk assessment. Both quantifiable and qualitative analysis can be performed to measure the current vulnerability status of the asset, as well as the effect of ongoing risk management improvements. Similarly, the return on investment of future actions can be forecast with some level of certainty. Vulnerability assessment considers the likelihood of a given scenario occurring by chance or intention. VA also postulates susceptibility and resultant damage.
## Appendix C: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAR</td>
<td>After Action Report/Implementation Plan (/IP)</td>
</tr>
<tr>
<td>AC</td>
<td>Area Command</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>CBP</td>
<td>Customs and Border Protection (DHS)</td>
</tr>
<tr>
<td>CDBG</td>
<td>Community Development Block Grant</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CIKR</td>
<td>Critical Infrastructure and Key Resources</td>
</tr>
<tr>
<td>CBO</td>
<td>Community-Based Organization</td>
</tr>
<tr>
<td>COG</td>
<td>Council of Government</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operations</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DOC</td>
<td>1) Department Operations Centers; 2) Department of Commerce</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DRC</td>
<td>Disaster Recovery Center</td>
</tr>
<tr>
<td>DRGR</td>
<td>Disaster Recovery Grant Reporting System</td>
</tr>
<tr>
<td>DRM</td>
<td>Disaster Recovery Manager</td>
</tr>
<tr>
<td>DSCA</td>
<td>Defense Support of Civil Authorities</td>
</tr>
<tr>
<td>EMAC</td>
<td>Emergency Management Assistance Compact</td>
</tr>
<tr>
<td>EOC</td>
<td>Emergency Operations Center</td>
</tr>
<tr>
<td>EOP</td>
<td>Emergency Operations Plan</td>
</tr>
<tr>
<td>EPA</td>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>ER</td>
<td>Emergency Relief Program</td>
</tr>
<tr>
<td>ESF</td>
<td>Emergency Support Function</td>
</tr>
<tr>
<td>ESFLG</td>
<td>Emergency Support Function Leadership Group</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>ETO</td>
<td>Emergency Transportation Operations</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration (DOT)</td>
</tr>
<tr>
<td>FBO</td>
<td>Faith-Based Organization</td>
</tr>
<tr>
<td>FCD</td>
<td>Federal Continuity Directive</td>
</tr>
<tr>
<td>FCO</td>
<td>Federal Coordinating Officer</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency (DHS)</td>
</tr>
<tr>
<td>FHWA</td>
<td>Federal Highway Administration (DOT)</td>
</tr>
<tr>
<td>FMCSA</td>
<td>Federal Motor Carrier Safety Administration</td>
</tr>
<tr>
<td>FRA</td>
<td>Federal Railroad Administration (DOT)</td>
</tr>
<tr>
<td>FRC</td>
<td>Federal Recovery Coordinator</td>
</tr>
<tr>
<td>FSE</td>
<td>Full-Scale Exercise</td>
</tr>
<tr>
<td>FTA</td>
<td>Federal Transit Administration (DOT)</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>HazMat</td>
<td>Hazardous Material</td>
</tr>
<tr>
<td>HMGP</td>
<td>Hazard Mitigation Grant Program</td>
</tr>
<tr>
<td>HND</td>
<td>Highways for National Defense</td>
</tr>
<tr>
<td>HUD</td>
<td>U.S. Department of Housing and Urban Development</td>
</tr>
<tr>
<td>HHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>HSEEP</td>
<td>Homeland Security Exercise Evaluation Program</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>HQ</td>
<td>Headquarters</td>
</tr>
<tr>
<td>IA</td>
<td>Individual Assistance</td>
</tr>
<tr>
<td>IAA</td>
<td>Interagency Agreement</td>
</tr>
<tr>
<td>IC</td>
<td>Incident Commander</td>
</tr>
<tr>
<td>ICP</td>
<td>Incident Command Post</td>
</tr>
<tr>
<td>ICS</td>
<td>Incident Command System</td>
</tr>
</tbody>
</table>
NVOAD  National Voluntary Organizations Active in Disaster
ODP    Office for Domestic Preparedness (DOJ)
OIG    Office of Inspector General
OIP    Office of Infrastructure Protection (DHS)
PA     Public Assistance Grant Program
PCII   Protected Critical Infrastructure Information Program
PHMSA  Pipeline and Hazardous Materials Safety Administration (DOT)
PNP    Private Nonprofit
PPE    Personal Protective Equipment
PSA    Protective Security Advisor
RETCO  Regional Emergency Transportation Coordinator
RETREP Regional Emergency Transportation Representative
RISC   Regional Interagency Steering Committee
RITA   Research and Innovative Technology Administration (DOT)
RPO    Regional Planning Organization
RRF    Ready Reserve Force
RSF    Recovery Support Functions
SCO    State Coordinating Officer
SEOC   State Emergency Operations Center
SME    Subject-Matter Expert
SOP    Standard Operating Procedure
SCC    Sector Coordinating Council
SRC    State Recovery Coordinator
SSP    Sector-Specific Plan
STRACNET Strategic Rail Corridor Network
STRAHNET Strategic Highway Network
TCRP   Transit Cooperative Research Program
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIM</td>
<td>Traffic Incident Management</td>
</tr>
<tr>
<td>TMC</td>
<td>Transportation Management Center</td>
</tr>
<tr>
<td>TRO</td>
<td>Transitional Recovery Office</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration (DHS)</td>
</tr>
<tr>
<td>TTX</td>
<td>Tabletop Exercise</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Command</td>
</tr>
<tr>
<td>USACE</td>
<td>U.S. Army Corps of Engineers (DoD)</td>
</tr>
<tr>
<td>USCG</td>
<td>U.S. Coast Guard (DHS)</td>
</tr>
<tr>
<td>VA</td>
<td>Vulnerability Assessment</td>
</tr>
<tr>
<td>VAL</td>
<td>Voluntary Agency Liaison</td>
</tr>
<tr>
<td>VOAD</td>
<td>Voluntary Agencies Active in Disaster</td>
</tr>
</tbody>
</table>