





UNDERSTANDING CRITICAL INFRASTRUCTURE DEPENDENCIES AND INTERDEPENDENCIES

INTRODUCTION

The systems that support US critical infrastructure sectors are becoming increasingly complex and interconnected, with multiple dependencies and interdependencies. For this reason, cyberattacks on these systems pose unique challenges to security and resilience. Disruptions to one sector can ripple through others, leading to more severe impacts. For example, malicious actors may target less secure systems that are connected to more critical ones, maximizing the effects of their disruption. By understanding how various systems, sectors, and subsectors interact, jurisdictions will be able to develop comprehensive incident response strategies that consider the potential ripple effects of an attack across interconnected infrastructures.

DEFINING DEPENDENCY AND INTERDEPENDENCY

Although the terms *dependency* and *interdependency* both describe connectedness between critical infrastructure systems and assets, they differ in connection directionality. See the following definitions:

Dependency 	Interdependency 
A unidirectional relationship in which one system depends on another for its operation. For example, the telecommunications sector depends on the power grid to function effectively.	A bidirectional relationship in which two systems mutually rely on each other. For example, the energy sector relies on water for extraction, processing, and cooling, and the water sector relies on energy to transport and treat water.

Dependencies and interdependencies can be categorized based on the type of connection:¹

- **Physical:** Direct reliance on another sector's output for functionality (e.g., telecommunications requiring electricity).
- **Cyber:** Dependence on information and data transmitted between systems (e.g., Supervisory Control and Data Acquisition (SCADA) systems that manage water treatment processes).

¹ Infrastructure Resilience Planning Framework, Cybersecurity and Infrastructure Security Agency, 2024.



- **Geographic:** Systems located near each other that are vulnerable to common disruptions (e.g., power lines and water pipelines sharing the same corridor).
- **Logical:** Regulatory, policy, or economic factors influencing operations (e.g., transportation affected by regional fuel policies).

STRATEGIES TO UNDERSTAND CRITICAL INFRASTRUCTURE DEPENDENCIES AND INTERDEPENDENCIES

As critical infrastructure continues to evolve in an increasingly complex environment, stakeholders across sectors will need to take proactive measures, such as the following, to safeguard public safety and maintain essential services:

- **Enhance communication and coordination.** Fostering collaboration across sectors is vital for improving situational awareness and response capabilities during emergencies, and establishing partnerships between public agencies and private entities is crucial for sharing information and resources.² Real-time information sharing, particularly concerning cyber threats, can significantly mitigate the cascading effects of a cyberattack on critical infrastructure.
- **Develop integrated emergency response plans.** Plans that explicitly address interdependencies among critical infrastructure systems are integral to preventing incidents and mitigating their consequences. These comprehensive plans should outline coordinated actions to take during disruptions, ensuring that all relevant sectors are prepared to respond effectively³ and that planned actions minimize adverse effects on critical infrastructure partners.
- **Invest in resilience measures.** Allocating resources to enhance the resilience of critical infrastructure systems includes upgrading aging infrastructure, implementing redundancy measures, and investing in technologies that improve operational efficiency.⁴ Such investments are vital for ensuring that critical services remain functional during emergencies.
- **Conduct scenario-based planning.** Engaging in exercises that simulate various disruption scenarios allows organizations to test the effectiveness of their response strategies. This approach helps organizations identify gaps in preparedness and informs necessary adjustments to existing plans.⁵

² National Infrastructure Protection Plan, Department of Homeland Security Cybersecurity and Infrastructure Security Agency, 2013.

³ "Electricity-Water Critical Infrastructure Interdependencies," National Association of State Energy Officials, 2021.

⁴ National Infrastructure Protection Plan, Department of Homeland Security Cybersecurity and Infrastructure Security Agency, 2013.

⁵ "Analysis of Critical Infrastructure Dependencies and Interdependencies," Argonne National Laboratory, 2015.



- **Conduct localized risk assessments.** The complexity of critical infrastructure systems makes it challenging to identify and analyze dependencies and interdependencies. By mapping out dependencies and interdependencies, jurisdictions can better understand their risk landscapes and conduct informed planning around potential vulnerabilities and outcomes. A structured risk assessment approach can help jurisdictions identify the complexities of critical infrastructure systems, especially given the increasing frequency and sophistication of cyber threats. Such an approach can enable organizations to systematically identify, evaluate, and prioritize vulnerabilities across interconnected sectors, which can help stakeholders understand cascading effects, prepare mitigation strategies, and allocate resources efficiently.

By adopting these proactive measures, stakeholders can better navigate the complexities of interconnected critical infrastructure systems and enhance their ability to prepare for a major cyberattack affecting critical infrastructure.

RISK ASSESSMENT METHODOLOGIES

To understand the risks from critical infrastructure dependencies and interdependencies, jurisdictions can conduct comprehensive risk assessments. A risk assessment framework provides a structured way to understand, predict, and mitigate the potential impacts from a cyberattack. Such an assessment involves mapping out dependencies and interdependencies across sectors and understanding how failures in one area can propagate through the system. Governmental and academic sources offer the following risk assessment methodologies that systematically identify and examine dependencies:

- Cybersecurity and Infrastructure Security Agency (CISA) [National Infrastructure Protection Plan](#)
- CISA [Infrastructure Resilience Planning Framework](#)
- [European Union Critical Infrastructure Protection Risk Assessment Methodology](#)
- Argonne National Laboratory [Analysis of Critical Infrastructure Dependencies and Interdependencies](#)
- [United Nations Office for Disaster Risk Reduction Critical Infrastructure Interdependency Analysis: Operationalizing Resilience Strategies](#)

Additional resources that may help jurisdictions accomplish their comprehensive risk assessments include the following:

- [National Institute of Standards and Technology Cybersecurity Framework](#), which includes risk assessment components that can be applied to assess dependencies and interdependencies in the context of cybersecurity.
- Department of Homeland Security (DHS) [Risk Lexicon](#), a unified vocabulary that DHS and its components use when communicating and sharing data.
- DHS [Critical Infrastructure Taxonomy](#), in which infrastructure assets are categorized at the sector, subsector, segment, subsegment, and asset levels.



In addition to the resources listed, the Blue Book Project team will be developing and distributing a risk mapping template for localities across the commonwealth to use to support a comprehensive critical infrastructure assessment process. This template will be described in a future white paper.

CONCLUSION

As a result of dependencies and interdependencies across critical infrastructure systems, a cyberattack on any single critical infrastructure sector can generate far-reaching consequences across multiple others. Understanding the complexities of critical infrastructure dependencies and interdependencies is vital for enhancing resilience against potential disruptions. By conducting thorough risk assessments, improving communication among stakeholders, developing integrated emergency response plans, investing in resilience measures, and utilizing scenario-based planning, jurisdictions can better prepare for and mitigate the risks associated with these interconnected systems.

Effective cross-sector risk management that is rooted in collaboration, redundancy, and real-time information sharing can reduce the severity of such disruptions and accelerate recovery efforts. Recognizing dependencies and interdependencies within critical infrastructure is vital for identifying vulnerabilities to cyberattacks, enhancing risk management strategies, informing resource allocation, and improving overall resilience against potential threats.