

# CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

PREPARE • PROTECT • MITIGATE • RESPOND • RECOVER



The Critical Infrastructure Resilience Institute (CIRI), led and managed by the University of Illinois at Urbana-Champaign, will conduct research and education to enhance the resiliency of the Nation's critical infrastructures and the businesses and public entities that own and operate those assets and systems.

With an emphasis on outputs-oriented research, education and workforce development, and early and continuous engagement with end users and homeland security practitioners, CIRI will explore the organizational, policy, business, and technical dimensions of critical infrastructure's dependence on cyber assets. CIRI will examine how computer hardware and software both contribute to and threaten resiliency and how industry makes decisions about cyber assets which contribute to resilience.

A Department of  
Homeland Security S&T  
Center of Excellence

EST. 2015

University of Illinois at  
Urbana-Champaign

Stanford University

Florida International  
University

Northeastern University

University of Washington

University of Southern  
California

University of Pennsylvania

Tennessee State University

Texas Tech University

Argonne National  
Laboratory

Sandia National  
Laboratories

## RESEARCH THEMES

### Understanding Resilient Critical Infrastructure Systems

Theme 1 research will yield an understanding of: the characteristics of resilient infrastructures; the scope and dynamics of the linkages and interdependencies of resilient infrastructures; and effective methods for bringing owners and operators of critical infrastructure together with the government sector to forge effective public/private partnerships to advance and enhance infrastructure security and resilience.

### Application of Critical Infrastructure in the Real World

Research activities of Theme 2 will focus on gaining a systems-level understanding of how critical infrastructure sectors are actually connected and how those interconnections affect risk management and risk sharing strategies used by industries and infrastructure owners and operators. Researchers will identify and evaluate policy and technology options that could support effective decision-making in collaborative risk management environments in real-world settings. Theme 2 research could lead to models allowing decision makers to effectively analyze questions such as: how do risk management strategies in one infrastructure community transfer risks to another?

### The Business Case for Infrastructure Resiliency

Theme 3 will seek an understanding of how businesses that own and/or operate critical infrastructure systems make decisions and tradeoffs regarding infrastructure security and resilience before, during, and after a catastrophic event. Researchers will also analyze government policies and regulations and the dynamics of risk insurance markets to determine their effects on the motivations and behavior of decision makers throughout the homeland security enterprise. Researchers hope to define future mechanisms that will properly incentivize decision makers to make timely and appropriate investments in infrastructure security and resilience.

### Future of Resilience

While considering the disruptive changes taking place in all sectors of the critical infrastructure as well as the constantly evolving threat landscape, Theme 4 researchers will seek breakthrough, game-changing, blue-sky projects that could significantly influence the adoption and evolution of critical infrastructure resilience. Research will involve the entire gamut of factors affecting security and resilience and the full resilience life-cycle. The goal of Theme 4 research is to gain an understanding of how resiliency can be designed and built into the physical and cyber infrastructures and the commercial and regulatory environments of the future.

[CIRI website](#)

TO ENGAGE WITH CIRI, [CONTACT: RANDY SANDONE](#)