National Infrastructure Protection Plan

State and Local Implementation

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security (DHS); Federal Sector-Specific Agencies; and other Federal, State, local, tribal, territorial, and private sector partners.

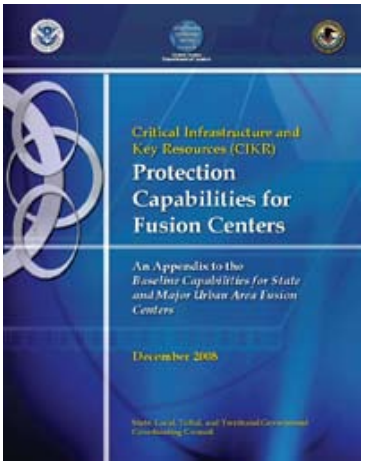
Implementation of the NIPP is one of the overarching priorities identified in the National Preparedness Guidelines. For NIPP partners at the State and local level, critical infrastructure and key resources (CIKR) protection programs form an essential component of homeland security strategies, particularly with regard to informing funding priorities and security investment decisions.

In accordance with the NIPP risk management framework, as well as the benchmarks and requirements identified in the Homeland Security Grant Program, State governments are responsible for developing, implementing, and sustaining a statewide/regional CIKR protection program. The processes necessary to implement the NIPP risk management framework at the State and/or regional level, including urban areas, should become a component of the State's overarching homeland security program, which should engage all relevant intergovernmental coordination points. Developing and managing a CIKR protection program for a given jurisdiction entails building an organizational structure and establishing mechanisms for communication and coordination among all CIKR partners.

State and regional CIKR protection programs should address all relevant aspects of CIKR protection and resiliency. The programs should leverage support from assistance programs that apply across the homeland security mission areas and cover all sectors present within the State and/or region and support national, State, and local priorities. State and local CIKR protection programs should also continuously share information between relevant public and private sector partners. Unique cybersecurity and geographical issues should be explicitly addressed, including trans-border concerns. Interdependencies among sectors and jurisdictions within those geographical boundaries must also be identified.

Critical Infrastructure and Key Resources Protection Capabilities for Fusion Centers

This document, released in January 2009, identifies the capabilities necessary for State and major urban area fusion centers to establish a CIKR analytic capability that supports CIKR protection activities at the State and local levels. This document is an appendix to the U.S. Department of Justice's

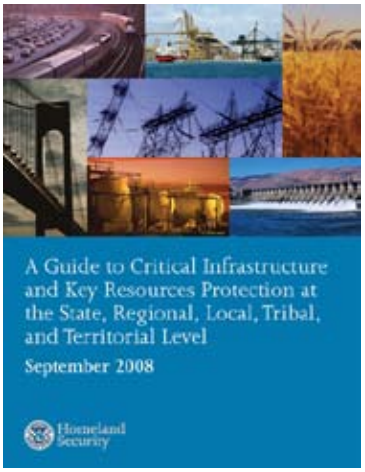


Global Justice Information Sharing Initiative's (Global) *Baseline Capabilities for State and Major Urban Area Fusion Centers* (*Baseline Capabilities document*), which defined the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions (e.g., the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information).

This document provides guidance for those fusion centers that have chosen to support CIKR protection activities. It identifies the additional capabilities fusion centers should achieve to effectively integrate CIKR activities into their analysis and information/intelligence-sharing processes and describes how the fusion center should support risk-reduction efforts taken by government and private sector partners. Additionally, this document communicates to Federal, State, local, and private sector officials the value in working with their local fusion center and articulates how they can better integrate their CIKR protection-related activities with the efforts of the fusion center.

A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level

DHS, in partnership with the State, Local, Tribal and Territorial Government Coordinating Council (SLTTGCC), released this document in September 2008. The guide builds on the tenets set forth in the NIPP by outlining the attributes, capabilities, needs, and processes that a State or other governmental entity should consider in establishing its own CIKR protection function that integrates with the NIPP and accomplishes the desired local benefits.



The guide is not intended to be prescriptive or to impose requirements on States, communities, or other CIKR partners. Rather, it suggests various strategies and leaves it to the discretion of each State, region, or locality to determine which approach(es) might be suited to their specific needs, operating environments, and risk landscapes. A variety of resources available to support State and local CIKR protection efforts are also described:

- Critical Infrastructure Warning Information Network (CWIN)
- Protected Critical Infrastructure Information (PCII) Program at www.dhs.gov/pcii
- CIKR Asset Protection Technical Assistance Program (CAPTAP) and Constellation/Automated Critical Asset Management System (C/ACAMS) at www.dhs.gov/acams
- Integrated Common Analytical Viewer (iCAV) at www.dhs.gov/iCAV
- TRIPwire, the Technical Resource for Incident Prevention, at www.tripwire-dhs.net
- Terrorism Risk Assessment Module (TRAM) Technical Assistance Program
- Maritime Assessment and Strategy Toolkit (MAST) Technical Assistance Program

Appendix 5A of the NIPP provides additional guidance for developing and implementing a State or regional CIKR protection program that can be adapted to reflect the variations in governance models across the States, recognizing that not all sectors are represented in each State or region.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.