Global Justice Information Sharing Initiative

United States Department of Justice

Critical Infrastructure and Key Resources (CIKR)

Protection Capabilities for Fusion Centers

An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

December 2008

State, Local, Tribal, and Territorial Government Coordinating Council

Critical Infrastructure and Key Resources (CIKR)

Protection Capabilities for Fusion Centers

An Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers*

December 2008

State, Local, Tribal, and Territorial Government Coordinating Council

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

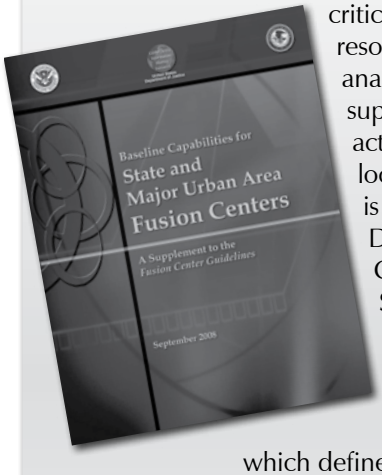
This project was supported by Grant No. 2007-NC-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Table of Contents

Introduction

Purpose

This document identifies the capabilities necessary for state and major urban area fusion centers (fusion centers) to establish a critical infrastructure and key resources (CIKR) protection analytic capability that supports infrastructure security 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, analyzing, and disseminating of terrorism, homeland security, and law enforcement information). One of the key principles of the *Fusion Center Guidelines* is that the mission of the center be developed locally and collaboratively to address the needs of the jurisdiction it is serving. Out of respect for that principle, the *Baseline Capabilities* document encourages but does not require centers to incorporate Critical Infrastructure Protection (CIP) activities into their mission. (See the *Baseline Capabilities* document, pages 1–3, for further background.)

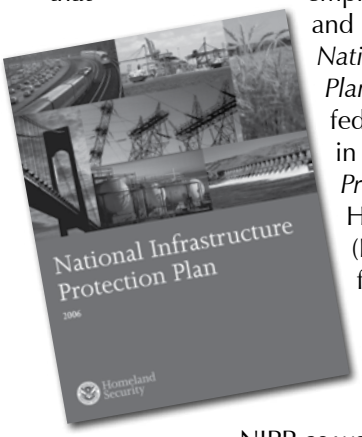


This document provides guidance for those fusion centers that have chosen to support CIP activities; it identifies the additional capabilities fusion centers should achieve in order to effectively integrate CIKR activities into their analysis and information/intelligence sharing processes and identifies how the center should support risk-reduction efforts taken by federal, state, local, and private sector partners.

This document also provides the federal, state, local, and private sector officials responsible for protecting CIKR with an overview of the value in working with their local fusion center and how they can better integrate their CIP-related activities with the efforts of the fusion center.

CIKR Protection Baseline Capabilities

It is recommended that every fusion center develop and integrate an analytic and information sharing capability that emphasizes the protection of regional and national CIKR in support of the *National Infrastructure Protection Plan* (NIPP)[1] and complementary federal, state, and local plans and in accordance with the *National Preparedness Guidelines* and the Homeland Security Grant Program (HSGP). This capability should facilitate multidisciplinary input from CIKR stakeholders and subject-matter experts (SMEs) into the risk management framework described in the NIPP, as well as integrate CIKR information into the routine intelligence cycle of the fusion center.



CIKR-related capabilities in the fusion center should center on the development of analytical products, such as risk and trend analysis. This analysis should combine CIKR-specific information with federal, state, and local criminal and homeland security information and intelligence and will contribute not only to the protection of CIKR but to the combined missions of federal, state, and local partners within each center. The capability should incorporate the dissemination of tailored, timely, and actionable analytical products related to CIKR, along with other fusion center products in order to maximize information sharing and support risk reduction activities of CIKR protection partners. The CIP capability should, through such efforts, be able to support a comprehensive understanding of the threat, local CIKR vulnerabilities, the potential consequences of attacks, and the effects of risk mitigation actions not only on the risk but also on business operations within the private sector.

Structure of the *Baseline Capabilities* Document

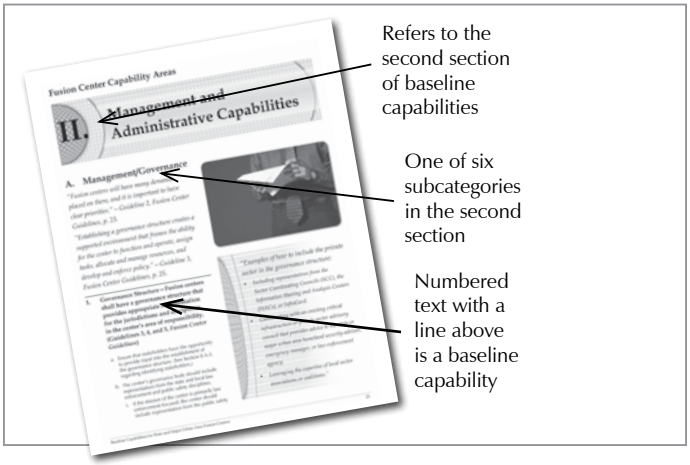
I. Fusion Process Capabilities

The intelligence cycle is defined in the *National Criminal Intelligence Sharing Plan* and incorporated into Guideline 1 of the *Fusion Center Guidelines*. For purposes of baseline capabilities, the titles are expanded to be:

A. Planning and Requirements Development
B. Information Gathering/Collection and Recognition of Indicators and Warnings
C. Processing and Collation of Information
D. Intelligence Analysis and Production
E. Intelligence/Information Dissemination
F. Reevaluation

II. Management and Administrative Capabilities

A. Management/Governance
B. Information Privacy Protections
C. Security
D. Personnel and Training
E. Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure
F. Funding



1 The NIPP is the comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies, and tribal partners. The NIPP lays out the plan for setting requirements for infrastructure protection, which will help ensure our government, economy, and public services continue in the event of a terrorist attack or other disaster. The purpose of the NIPP is to "build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency." The NIPP was released on June 30, 2006.

I. Fusion Process Capabilities

The capabilities outlined below are designed to be integrated with all other fusion process capabilities to assist fusion centers in achieving their mission. They are organized to correlate with and complement the *Baseline Capabilities* document. For the sake of brevity and clarity, only those items that are unique to CIKR are included in this document; it is assumed that the fusion center is adhering to the baseline capabilities listed in the *Baseline Capabilities* document.

The following capabilities address the plans and their associated policies, standards, and processes and procedures (collectively "procedures") needed to enable various aspects of the Fusion Process: the gathering, processing, analyzing, and disseminating of terrorism, homeland security, and law enforcement information. For these capabilities to be considered achieved or accomplished, the plans and procedures should be documented and provided to appropriate center personnel and partners. (See *Baseline Capabilities* document for further information.)

A. Planning and Requirements Development

1. Fusion centers shall ensure that relevant CIKR information and analysis are included in the required statewide/ regional risk assessment that identifies and prioritizes threats, vulnerabilities, and consequences within a given region and is conducted at regular intervals, in support of the *Baseline Capabilities* Requirements process. [See BC #I.A.2.]

2. Fusion centers shall ensure that CIKR information requirements are developed as a part of the regular information requirements process. [See BC #I.A.3.]

3. For each of the primary information flows identified in Section I.A. of the *Baseline Capabilities* document (e.g., Suspicious Activity Reporting (SAR); Alerts, Warnings, and Notifications, and Situational Awareness Reporting), fusion centers shall incorporate their core and ad hoc CIKR stakeholders (as defined in Section II. A. below) into their plans and procedures. [See BC #I.A.4., 5., 6.]

4. Fusion centers shall identify and have access to CIKR-related data resources and repositories that are needed to conduct analysis based on the mission of the center, the findings of the statewide or regional risk assessment, and the center's defined Information Requirements. [See BC #I.A.7.][2] Following completion of required U.S. Department of Homeland Security (DHS) training, the system(s),

2 Refer to BC II.E. on guidance to further develop plans for access to data sources based on the fusion center's defined mission and core business process.

such as the Constellation/Automated Critical Asset Management System (C/ACAMS[3]), shall provide users with the ability to:

a. Collect, store, and share classified and unclassified CIKR data.

b. Collect data via secure means, either remotely at CIKR sites or locally at fusion centers.

c. Allow limited access to private sector entities, in accordance with established legal frameworks (such as the Protected Critical Infrastructure Information [PCII] program),[4] to facilitate data collection directly from CIKR owners and operators.

d. Access a comprehensive set of tools and resources to develop and implement critical infrastructure programs.

e. Allow the user to manage the collection and effective use of CIKR-related data.

f. Focus on pre-incident prevention and protection but also assist in post-incident response and recovery operations.

---

5. Fusion centers shall support CIKR-related exercises conducted by federal, state, and regional officials or organizations responsible for Critical Infrastructure Protection activities, in order to validate the center's operations, policies and procedures, and training activities and shall develop action plans to mitigate any identified gaps. [See BC #I.A.10.]

B. Information Gathering/ Collection and Recognition of Indicators and Warnings

---

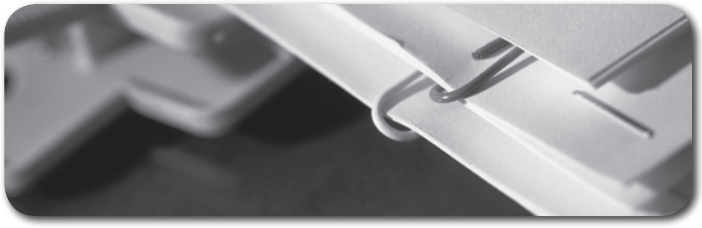
1. Fusion centers shall incorporate CIKR information requirements and stakeholders into their information gathering and reporting strategy with a particular emphasis on clearly defined processes for CIKR partners to report information to the fusion center in a manner that is consistent with the center's privacy policy. [See BC #I.B.1.]

---

2. Fusion centers shall review and, as necessary, update their policies, processes, and mechanisms that are used for receiving, cataloging, and retaining information provided to the center (as called for by BC #I.B.3.), to ensure that CIKR-related information is appropriately stored and protected.

3 See page 16 for background on the Constellation/Automated Critical Asset Management System (C/ACAMS).

4 The Protected Critical Infrastructure Information (PCII) program offers protection for critical infrastructure information voluntarily shared with government entities for homeland security purposes. See page 17 for more details.



C. Processing and Collation of Information

1. "Processing and collation involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined." —Guideline 1, *Fusion Center Guidelines*, p. 20. Please refer to the *Baseline Capabilities* document for more information on processing and collation of information, including CIKR-related information. [See BC #I.C.]

D. Intelligence Analysis and Production

1. Fusion centers shall update their production plans, as called for in Section I.D.1. of the *Baseline Capabilities* document, to incorporate CIKR-related analysis and develop products for CIKR stakeholders that enhance the protection of critical infrastructure.

2. Consistent with Section I.D.7. of the *Baseline Capabilities* document, fusion centers shall consider assigning at least one analyst to the CIKR analysis function on a full-time basis.

3. Fusion centers shall establish processes to utilize the information collected from security partners and other sources to inform the assessment of security risks and enhance the protection and resiliency of critical infrastructure. To accomplish this, fusion centers shall provide the necessary CIKR tools and resources for analysis of information and data. The following resources should be integrated in a way that facilitates the processing, integrating, and analyzing of CIKR information: [See BC #I.D.8.]

a. Geographic, jurisdictional, and/or sector inventories

b. Voluntary submittals from security partners

c. Site assistance visits/comprehensive reviews

d. Sector-specific assessment tools

e. Results of studies

f. Periodic data calls

g. Pre-incident response plans

h. Open source information and intelligence

i. Classified information and intelligence (at the classification level of the fusion center)

4. CIKR analysts shall work in partnership with other analysts, local law enforcement, public safety and emergency response personnel, DHS Protective Security Advisors (PSAs), and the private sector to integrate and analyze information and intelligence received into timely and actionable intelligence that is tailored to the protection of CIKR. Analysts shall:

a. Use various analytical techniques and conduct appropriate analysis (which may include risk, target, and trend analysis).

b. Evaluate and analyze raw CIKR data to draw conclusions related to vulnerabilities and consequences.

c. Liaise with CIKR partners and other agencies to identify emerging threats, deconflict information, and support the development of routine information bulletins and special events threat assessments. Integrate analyses of CIKR with intelligence from various sources to develop timely, actionable CIKR information products.

d. Leverage federal, state, and local data collection and warehousing efforts, through programs such as C/ACAMS, to collaborate across jurisdictions and geographic regions to integrate national-level data with state and local information.

e. Strive to produce CIKR products at the lowest practical classification level to ensure maximum usefulness for partners without security clearances.

f. Be collocated with other analysts within the fusion center.

g. Track and monitor suspicious activity reports (SARs) to identify behavior or incidents that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.

   i. Consistent with Section I.A.4., *Baseline Capabilities* document, ensure that SARs which are determined to be Information Sharing Environment-SARs (ISE-SAR) are documented in the ISE-SAR Functional Standard format and posted in the appropriate ISE Shared Space.

5. CIKR analysts shall assist the fusion center with providing situational CIKR awareness and helping to inform senior leadership decision making. Analyst responsibilities are to:

a. Provide complete situational awareness to all appropriate federal, state, and local response authorities.

b. Serve as a coordination hub to deconflict incoming information and intelligence from all sources and bring together CIKR-related prevention, preparedness, protection, response, and recovery authorities, capacities, and resources among local jurisdictions, across sectors, and across regional entities.

c. Participate in multidirectional information flow between government and private sector security partners and integrate federal, state, local, tribal, and private sector security partners, as appropriate, into the intelligence cycle.

6. Conduct CIKR-related emergency management/contingency planning.

a. Provide analysis to support emergency management and contingency planning, particularly in the areas of restoration and reconstitution of state and nationally significant assets and networks.

b. Develop plans and policies for use during an event to provide support to the state or local Emergency Operations Center and/or Joint Field Office in accordance with the National Incident Management System (NIMS).

7. Fusion centers shall coordinate with federal, state, local, and private sector security partners to ensure that CIKR-specific risk assessments are conducted in order to develop a sophisticated understanding of the risk to CIKR.

a. Support the ability to determine private sector vulnerabilities, anticipated precursor activities, anticipated adversary tactics, techniques and procedures, potential consequences of terrorist attacks or natural hazards, and lessons learned from overseas terrorist activities.

b. Ensure that the methodologies used are credible and, when possible, that they are comparable to the NIPP Baseline Criteria for Assessment Methodologies.[5]

5 The NIPP specifies the baseline criteria for methodologies used to support all levels of comparative risk analysis under the NIPP framework. Many owners and operators have performed vulnerability and/or risk assessments on the assets, systems, and networks under their control. To take advantage of these activities, DHS and the sector-specific agencies use the results from previously performed assessments wherever possible. However, the assessment work to date has varied widely both within and across sectors in terms of its assumptions, comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies, and other characteristics. In order to use previous assessment results to support national comparative risk analysis, the methodologies used to perform the assessments must be tested against the NIPP baseline criteria. See the NIPP, Appendix #3A, for more information.

8. In addition to the requirements for analyst training outlined in Section I.D.3. of the *Baseline Capabilities* document, designated CIKR analysts shall be trained in all relevant analytic and information protection regulations, procedures, and considerations to ensure that critical infrastructure and private sector information is appropriately gathered, processed, analyzed, disseminated, protected, and secured.

a. Training shall include:

i. Specialized CIKR training.[6]

ii. Use of CIKR data resources and analysis tools, such as C/ACAMS.

iii. CIKR vulnerability and risk assessment tools and methodology.

iv. Risk/target/trend analysis techniques.

v. An overview of the NIPP and its risk management framework.

vi. All relevant CIKR information protection regulations, procedures, and considerations, to include Protected Critical Infrastructure Information (PCII).

E. Intelligence/Information Dissemination

1. Fusion centers shall incorporate CIKR stakeholders into the dissemination plan required by Section I.E.1., *Baseline Capabilities* document.

a. Identify the processes and protocols for ensuring CIKR information is disseminated to appropriate government authorities and CIKR owners and operators consistent with the preestablished procedures for sharing such information in a manner consistent with all applicable legal frameworks.

b. Ensure appropriate information resulting from any of the fusion center's analytic products is provided to affected industry sectors.

2. Consistent with Section II.E.3., *Baseline Capabilities* document, fusion centers shall ensure relevant CIKR analysis is reported to DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the FBI Field Intelligence Group (FIG), and other appropriate federal agencies.

a. Establish mechanisms to coordinate and reconcile CIKR information and intelligence and associated recommendations for CIKR protection and resiliency with other fusion center products.

b. Maintain such mechanisms to contribute information of value to ongoing federal and national-level assessments of terrorist risks.

6 The SLTTGCC is currently working with the DHS Office of Infrastructure Protection to create a CIKR-specific training curriculum for analysts.

3. Fusion centers shall develop technology-assisted methods to distribute CIKR information and intelligence to appropriate government authorities and CIKR owners and operators. The fusion center shall ensure that:

a. Technology-assisted dissemination used is appropriate for the level of classification.

b. Unclassified distribution utilizes technologies that have become ubiquitous and easy to use for all recipients.

c. The technology utilized is accepted by CIKR partners. Examples would include:

   i. Constellation/Automated Critical Asset Management System (C/ACAMS)

   ii. Homeland Security Information Network – Critical Sectors (HSIN-CS)

   iii. Homeland Security Information Network – Intelligence

   iv. Homeland Secure Data Network (HSDN)

   v. Law Enforcement Online (LEO)

F. Reevaluation

1. In accordance with the *Baseline Capabilities* document (Section I.F.), fusion centers shall integrate a feedback mechanism (such as Technology Acceptance Modeling[7]) to evaluate the overall effectiveness of CIKR information/intelligence sharing into their products. Analysts shall encourage recipients of their products to provide feedback, such as:

a. Have products reached them in a timely manner?

b. Do they believe the products to be accurate?

c. Have the products motivated them to take concrete actions?

d. Do the products contain appropriate contextual background?

e. Do they believe the producer of the products is credible and trustworthy?

f. Does the product address an anticipated event?

7 University and private sector research has demonstrated that Technology Acceptance Modeling (TAM) is a statistically validated method of predicting "loyal use" of a product. As fusion centers continue to improve intelligence products with the intention that stakeholders become "loyal users" of their products, providing a product that is perceived as "useful" in the six Technology Acceptance Modeling variables (questions) can provide ongoing feedback on this critical factor. If products are not perceived as useful by stakeholders, no matter how good the intelligence, stakeholders will not regularly utilize the products.

II. Management and Administrative Capabilities

A. Management/Governance

1. Fusion centers shall provide a mechanism for representatives of CIKR stakeholders to participate in the governance process in at least an advisory capacity. [See BC #II.A.1.]

2. Fusion centers shall review and update their mission statement to ensure that it appropriately conveys the purpose, priority, and roles of the center as it relates to support CIKR protective activities. [See BC #II.A.2.]

3. Consistent with Section II.A.3. of the *Baseline Capabilities* document, fusion centers, in partnership with the state or major urban area official or organization responsible for CIP activities, shall identify the CIKR organizations that represent their core (permanent) and ad hoc stakeholders (including Sector Coordinating Councils, Information Sharing Advisory Councils [ISACs] and Infragard Chapters), as well as the roles and responsibilities for each stakeholder, and develop mechanisms and processes to facilitate a collaborative environment with these stakeholders.

a. As an initial step, document the sites and sector types of the CIKR located within the fusion center's geographic area of responsibility.

b. Fusion center support to sites and sectors shall be prioritized based on risk and the guidance of state and/or major urban area officials responsible for CIP activities and the DHS Protective Security Advisor.

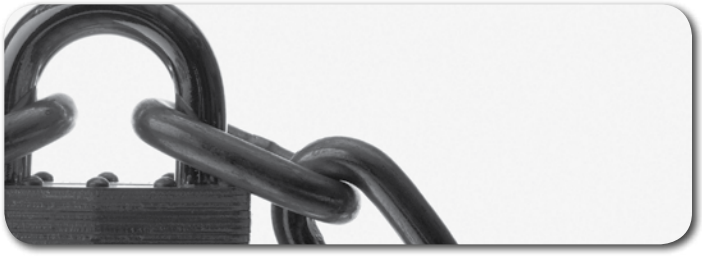
c. Follow all procedures outlined in Section II.A.3. of the *Baseline Capabilities* document for each stakeholder, particularly the requirements for a Memorandum of Understanding (MOU) and, if necessary, a Nondisclosure Agreement (NDA).

d. Information exchange between fusion centers and security partners shall include information pertaining to:
   i. Site-specific security risks.
   ii. Inter- and intrasector interdependencies.
   iii. Suspicious activity reports.
   iv. Adversary tactics, techniques, and procedures.
   v. Best practices in CIKR protection and resiliency.
   vi. Standard operating procedures for incident response.
   vii. Emergency communications capabilities.
   viii. Emergency contact/alert information.

4. **Fusion centers shall review and update their policies and procedures manual, to ensure that CIKR-related goals, policies, rules, and regulations are reflected in the manual.**

B. Information Privacy Protections

1. **Fusion centers shall review and update their privacy policy to ensure that the incorporation of CIKR information and analysis into their business processes is done in a manner that protects the privacy, civil liberties, and other legal rights of individuals, including U.S. corporations, protected by applicable law to include PCII. [See BC #II.B.]**



C. Security

1. **Fusion centers shall review and update their security plan to support the incorporation of CIKR information and analysis into the fusion center's business processes. [See BC #II.C.]**

D. Personnel and Training

1. **Fusion center managers shall update the staffing plan and training plan to support the incorporation of CIP information and analysis into the fusion center's business processes. [See BC #II.D.]**

E. Information Technology/ Communications Infrastructure, Systems, Equipment, Facility, and Physical Infrastructure

1. **Fusion centers shall review and update their information technology and communications plans, infrastructure, systems, equipment, and contingency and continuity of operations plans to support the incorporation of CIKR information and analysis into the fusion center's business processes. [See BC #II.E.]**

2. The CIP capability should ensure that the system(s) utilized allow a broad and secure exchange of sensitive but unclassified CIKR information between federal agencies, owners and operators, and state and local governments (an example would be HSIN-CS[8]). The system(s) should be able to:

a. Receive, submit, and discuss timely, actionable, and accurate CIKR information.

b. Communicate information pertaining to threats, vulnerabilities, security, and response and recovery activities affecting sector and cross-sector operations.

c. Maintain a direct, trusted channel with CIP stakeholders.

d. Access a source for infrastructure protection alerts, information bulletins, and analysis related to individual sectors.

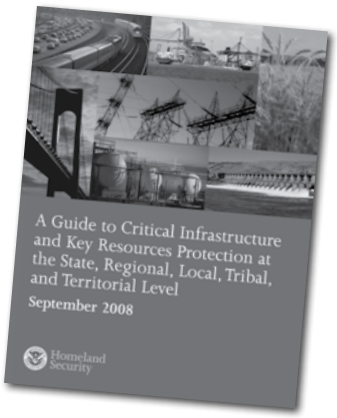
e. Engage in secure discussions and document sharing with CIP partners.

f. Contribute to and benefit from strategic and tactical information sharing on an ongoing/ periodic basis.

g. Access timely information on recommended pre-incident prevention and preparedness best practices and activities.

F. Funding

No additional capabilities are required.



Consider the applicability of DHS preparedness grant programs, as well as targeted infrastructure protection-focused grant programs, as described in Appendix A of the DHS/SLTTGCC's *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level*.

8 See page 15 for more information on the Homeland Security Information Network-Critical Sectors (HSIN-CS).

Fusion Center CIKR Operations

As discussed, a primary function of the CIKR capability is to fuse threat, vulnerability, and consequence data by combining national and local intelligence, private sector CIKR-specific information related to vulnerability and risk, and law enforcement information. These activities describe the elements of the information and intelligence cycle that define fusion center operations. The CIKR capability must become an integral component in the information and intelligence cycle of the fusion center. The information and intelligence cycle is a process for systematically collecting, evaluating, and disseminating information and intelligence obtained by the fusion center, and the CIKR capability must be integrated throughout all aspects of this process. The steps in the information and intelligence cycle, as described in the *Baseline Capabilities* document, are described below.

Step 1: Planning and Requirements Development

The first step is ascertaining the current capabilities and CIKR requirements of stakeholders and then developing a coordinated plan that assigns responsibilities for collecting and/or producing CIKR intelligence that meets the requirements of those stakeholders. This plan usually takes the form of a requirements list that specifies what kind of information needs to be collected and what intelligence products would meet those requirements.

Step 2: Information Gathering/Collection

Collection involves the purposeful acquisition of raw CIKR-related information from which an intelligence product will be produced. Collection activity begins with the identification and assessment of strategies and methods that will yield the information necessary to meet the intelligence requirements. This will enable the CIP capability in a fusion center to develop and organize collection systems and commence actual collection of CIKR data. Baseline collection plans are ideally prepared in advance of an incident or issue, are best developed through collaboration between the producers of information and the ultimate end users, and provide a guideline to expedite the CIKR analyst actions at the onset of an incident.

The collection process for CIKR information involves using various open and protected sources. Examples include the use of existing state fusion center records or databases, open source searches, site assistance visits, technical systems, federal and state government resources, subject-matter experts, utilization of associations (including Sector Coordinating Councils), and information shared by the CIKR/private sector, to include suspicious activity reports.

Step 3: Processing and Collation of Information

Processing and collation of CIKR-related information involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined, as well as a review of the collected and evaluated CIKR-related information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

Step 4: Intelligence Analysis and Production

Intelligence analysis and production refer to the process of evaluating and transforming the CIKR information into descriptions, explanations, and conclusions for the consumers. The activities associated with this step involve, among other things, the arrangement by subject matter (e.g., specific CIKR sector) and data reduction. It is also

during this phase that CIKR data is studied, evaluated, and abstracted to create a product that meets the requirements previously identified. The analysis involves the formulation of hypotheses, testing them with data, and integrating the results into explanations, assessments, and forecasts or early warning. The analysis of information is necessary to produce intelligence.

Step 5: Intelligence/ Information Dissemination

Once analysis is completed, the finished CIP intelligence product is then disseminated to the consumers to prepare, protect, mitigate, or respond to threats targeting their CIKR asset using different tear-line reports,[9] as appropriate.

Step 6: Reevaluation

The final step involves the CIKR analysts leading the evaluation of both the efficacy of the process and the value of the intelligence derived from the process. This evaluation and feedback informs the improvement of the cycle for future actions.

Integrating the CIKR capability into state and local fusion centers will aid in the development of products that enable and support federal, state, local, and private sector decision making.

The steps in this CIKR intelligence cycle are shown below:

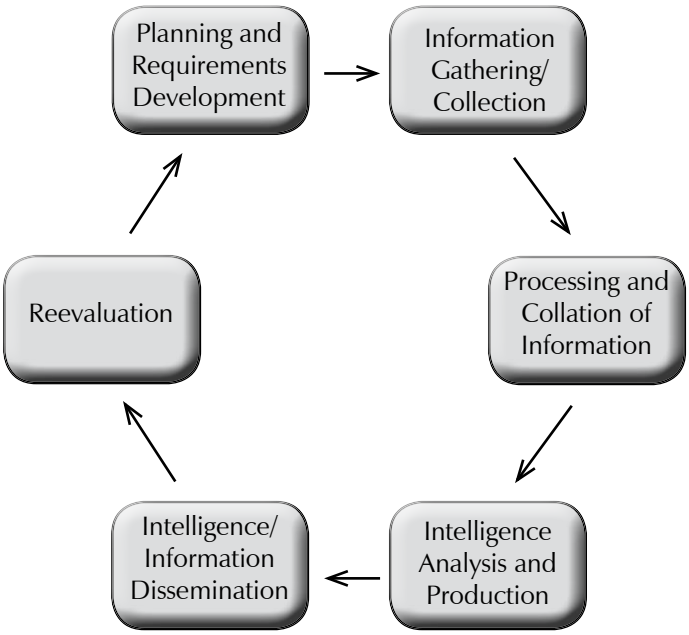


Figure 1—The CIKR Intelligence Operations Cycle

9 A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the "tear line" can be released as sensitive but unclassified.

Available Resources

This section provides an overview of relevant resources available to support the CIKR fusion center function under the NIPP sector partnership model.

The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

The SLTTGCC, under the NIPP, serves as a forum to ensure that state, local, tribal, and territorial homeland security officials or their designated representatives are integrated fully as active participants in national CIKR protection efforts. The SLTTGCC provides the organizational structure to coordinate across jurisdictions on state and local-level CIKR protection guidance, strategies, and programs.

The U.S. Department of Homeland Security (DHS)

DHS seeks to prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. To advance this objective, DHS has developed both the NIPP and the *National Response Framework* (NRF).

The NIPP is the comprehensive risk management framework that clearly defines critical infrastructure protection roles and responsibilities for all levels of government, private industry, nongovernmental agencies, and tribal partners. The NIPP lays out the plan for setting requirements for infrastructure protection, which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster. The purpose of the NIPP is to "build a safer, more secure, and more resilient America by enhancing protection of the Nation's CIKR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."

The NRF defines the principles, roles, and structures that organize how we respond to an event as a nation. The NRF:

- Describes how communities, tribes, states, the federal government, private sectors, and nongovernmental partners work together to coordinate national response.
- Describes specific authorities and best practices for managing incidents.
- Builds upon the NIMS, which provides a consistent template for managing incidents.

There are a number of components within DHS that help facilitate the objectives of the NIPP and the NRF at the regional, state, and local levels. These components provide various resources to security partners. The DHS components and their spectrum of applicable resources are listed below.

Office of Intelligence and Analysis (I&A)

I&A is the executive agent for the State and Local Fusion Center Program within the U.S. Department of Homeland Security. Its objective is to create partnerships with fusion centers and major cities to improve information flow between DHS and the centers and improve the effectiveness of the centers as a network. I&A leads the DHS effort to provide people and tools to the fusion centers to create a web of interconnected nodes across the country—creating a national fusion center network with analytic centers of excellence nationwide.

I&A has many valuable resources that could be tapped by a fusion center's CIP capability. They include:

- Ability to provide fusion centers with the national threat perspective, warning information, and responses to requests for information.
- DHS information technology and data network access (HSIN-Intel, HSDN).
- Ability and tools to assess threats via multilevel government participation, meshing domestic on-the-ground knowledge with overseas intelligence.
- Security clearances for state/locals, facility certification, and COMSEC equipment maximizing sharing of classified intelligence.
- Training courses for intelligence and analysis, including:
  - Civil rights, civil liberties, and privacy
  - Introductory analytic tradecraft
  - Analysis and critical-thinking skills
  - Open source tradecraft and technology
- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). HITRAC is DHS's Intelligence-Infrastructure Protection Fusion Center, composed of analysts from both the Office of Infrastructure Protection (IP) and I&A. Together, these analysts execute the infrastructure risk assessment responsibilities created by the Homeland Security Act of 2002, serving federal, state, local, and owner-operator requirements for threat and risk-based infrastructure analysis. HITRAC programs and products include:
  - Sector-Specific Threat Assessments
  - Sector-Specific Risk Assessments
  - Individual State Threat Assessments
  - Tier 1/Tier 2 List
  - Strategic Homeland Infrastructure Risk Assessment (SHIRA)
  - Critical Infrastructure Red Team

Office of Infrastructure Protection (IP)

IP is the lead agency in the national effort to reduce risk to CIKR assets. IP recognizes that fusion centers provide a capability that can be leveraged to better facilitate CIP practices and to enhance resiliency and the security posture of CIKR at the regional level. In addition, IP can be a valuable partner to fusion centers. IP can complement fusion centers with resources that will improve the security and delivery of services to regional stakeholders.

IP's strengths include data collection and management tools; risk analytic and modeling, simulation, and analysis capabilities, methodologies, and products; and the ability to maintain relationships with national CIKR partners through the Sector Partnership Framework.

IP can offer fusion centers a suite of services through its products and resources. These services will enable the fusion centers to build their CIKR protection capabilities more effectively. IP has the following national-level core assets that are available for fusion centers, which meet criteria set forth in this document, and can be utilized by incorporating them into already existing capacities at fusion centers:

- **Homeland Security Information Network-Critical Sectors (HSIN-CS)** is the primary technology tool used to facilitate the information sharing necessary for coordination, planning, mitigation, and response within the CIKR Sector Partnership. HSIN-CS is an Internet-based platform that enables secure, encrypted CUI-level communications between DHS and vetted members of the CIKR sectors as well as within and across the sectors. DHS fully funds and maintains HSIN-CS for eligible members of the CIKR sectors, thereby removing the obstacles of cost and day-to-day effort required to support systems implementation, operations, and maintenance. HSIN-CS includes a separate site for each CIKR sector, designed and implemented in collaboration with the sector's Government Coordinating Council and Sector Coordinating Council in order to best meet sector-specific needs. It also provides a top-level publishing capability to share applicable DHS and other information resources with all sectors simultaneously. These key characteristics of HSIN-CS directly support the building of trusted, reliable, and valued public-private sector partnerships, as well as two-way sharing of information.
- **Constellation/Automated Critical Asset Management System** (C/ACAMS) is a secure, Web-based portal designed to help state and local first responders, emergency managers, and homeland security officials collect and organize CIKR asset

data as part of a comprehensive CIKR protection program. C/ACAMS was developed in partnership with the Los Angeles Police Department's Operation Archangel and the Federal Emergency Management Agency's National Preparedness Directorate. C/ACAMS is provided free for state and local use.

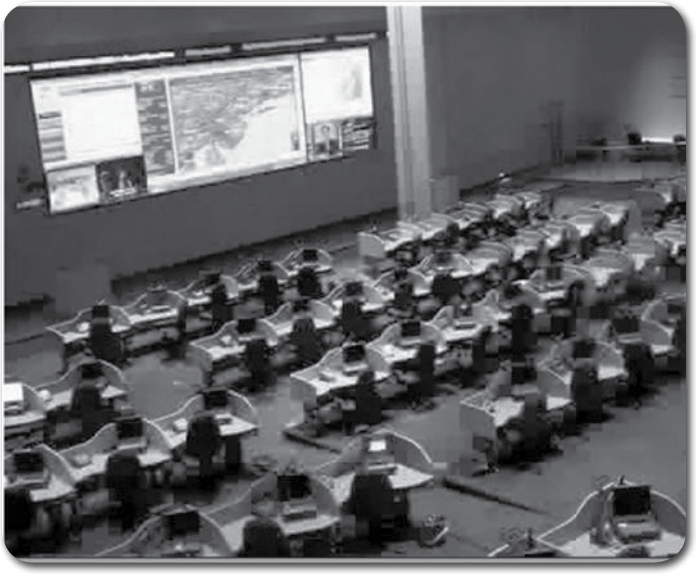
- **Protective Security Advisor (PSA)**—The PSA program was established to better partner with state governments, local communities, and businesses to assist with local efforts to protect critical assets. The PSA mission is to represent DHS and IP, working with state Homeland Security Advisor (HSA) offices and their security partners throughout the region and serving as liaisons among DHS; the private sector; and federal, state, territorial, local, and tribal entities. PSAs act as DHS's on-site critical infrastructure and vulnerability assessment specialists. During natural disasters and contingency events, PSAs work in state and local Emergency Operations Centers (EOCs) and provide expertise and support to the IP Infrastructure Liaison Cell, working to support the Principal Federal Official (PFO) and Federal Coordinating Officer (FCO) responsible for domestic incident management. Additionally, PSAs provide support to officials responsible for special events planning and exercises and provide real-time information on facility significance and protective measures to facility owners and operators and state and local representatives.
- **CIKR Asset Protection Technical Assistance Program (CAPTAP)**—The CAPTAP is offered jointly by IP and FEMA's National Preparedness Directorate to assist state and local first responders, emergency managers, and homeland security officials in understanding:
  - The basic tenets of the NIPP.
  - The value of a comprehensive state and local infrastructure protection program.
  - The steps required to develop and implement such a program.

  The CAPTAP curriculum also includes instruction on the use of the C/ACAMS as a tool to support infrastructure protection programs.[10]
- **Protected Critical Infrastructure Information (PCII)**—The PCII program was created by Congress under the Critical Infrastructure Information (CII) Act of 2002. It offers protection to CII voluntarily shared with government entities for homeland security purposes. Typically, when information is shared with the federal government, it becomes a public record and may be accessed through public disclosure laws, unless additional protections are applied. The PCII program works with various government partners to integrate PCII protections into their data collection processes. This offers a way for government security analysts to access CII, while owners/operators of critical infrastructure are assured that their information is protected from public disclosure. Program safeguards ensure that only trained and authorized individuals, with a need to know can access PCII and use it only for homeland security purposes.
- **Integrated Common Analytical Viewer (iCAV)**—iCAV is a geospatial-intelligence analytic tool that unites homeland security mission partners through an integrated Web-based Service-Oriented Architecture for information dissemination, analysis, and visualization. iCAV provides a geospatial context for situational and strategic awareness across the nation and around the globe to better prepare for, prevent, respond to and recover from natural and man-made disasters.
- **National Infrastructure Coordinating Center (NICC)**—The NICC serves as the 24/7 operational communication and coordination hub for CIKR sectors and DHS. It provides situational and operational awareness across the CIKR sectors and also provides a central point for requests for information and action for the CIKR sectors. The NICC also has operational responsibility for DHS content update of HSIN-CS portals and maintains a registry and official lists of sector partnership contacts for notifications and alerts.
- **Technical Resource for Incident Prevention (TRIPwire)**—TRIPwire is DHS's online, collaborative information sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist improvised explosive device (IED) tactics, techniques, and procedures, including design and emplacement considerations. Developed and maintained by the DHS Office for Bombing Prevention (OBP), the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement to anticipate, identify, and prevent IED incidents.

IP resources also offer analytic resources and products that can be used as references by fusion centers to further their own analysis and develop new analytic products and programs. These resources include:

- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)**—HITRAC is the U.S. Department of Homeland Security's Intelligence-Infrastructure

10 PCII training is a prerequisite to the CAPTAP training.



Protection Fusion Center, composed of analysts from both the IP and I&A. Together, these analysts execute the infrastructure risk assessment responsibilities created by the Homeland Security Act of 2002, serving federal, state, local, and owner-operator requirements for threat and risk-based infrastructure analysis. HITRAC programs and products include:

- Sector-Specific Threat Assessments
- Sector-Specific Risk Assessments
- Individual State Threat Assessments
- Tier 1/Tier 2 List
- Strategic Homeland Infrastructure Risk Assessment (SHIRA)
- Critical Infrastructure Red Team

- **National Infrastructure Simulation and Analysis Center (NISAC)**—The NISAC is DHS's congressionally mandated modeling, simulation, and analysis program. The center prepares and shares analyses of critical infrastructure and key resources (CIKR), including their interdependencies, consequences, and other complexities. NISAC provides three types of products: preplanned long-term analyses, preplanned short-term analyses, and unplanned priority analytical projects as directed by the Assistant Secretary for Infrastructure Protection. NISAC products provide essential insight for mitigation design and policy planning and address the cascading consequences of infrastructure disruptions across all 18 CIKR sectors at national, regional, and local levels.

Federal Emergency Management Agency (FEMA)/National Preparedness Directorate (NPD)

In coordination with I&A and the U.S. Department of Justice's Bureau of Justice Assistance, the NPD offers many valuable resources that are currently leveraged by fusion centers and could be leveraged by the CIP capability within a fusion center. They include:

- Fusion Process Technical Assistance (130+ technical assistance deliveries already made to support state and local fusion center efforts).
- Various training programs (thousands of state/local officials have already participated in DHS-sponsored or -approved training).

FEMA Grant Programs Directorate (GPD)

- Grant funding (more than $250 million has already been provided to states and urban areas between fiscal year FY2004 and FY2007 in support of intelligence and information sharing activities).

Federal Bureau of Investigation (FBI)

The FBI supports the protection of CIKR through InfraGard, a multifaceted public/private outreach program with more than 26,000 members in 86 chapters nationwide. All 56 FBI field offices support at least one InfraGard Chapter through the assignment of Special Agent InfraGard Coordinators. InfraGard maintains partnerships with the FBI's Directorate of Intelligence, Counterterrorism Division, Counterintelligence Division, Criminal Investigative Division, and Weapons of Mass Destruction Directorate, as well as information sharing and/or partnerships with multiple other agencies, particularly with DHS.

The primary focus of InfraGard is to share actionable intelligence information, which is made possible through a formalized membership vetting process. The vetting of each InfraGard member has allowed individual FBI field divisions to utilize this membership to enhance investigative and intelligence capabilities in their respective divisions. InfraGard maintains communication via physical meetings within each chapter; a public Web site; and a secure, clientless virtual private Web site, which is populated daily with critical infrastructure-related intelligence community products and information designed to educate and enable InfraGard members. Further information can be obtained from www.infragard.net.

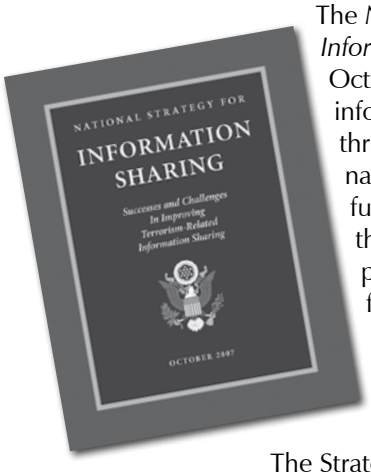
The Path Forward

Ultimately, protection and preparedness can be only as good as the CIKR information and intelligence made available to the engaged security partners. The approach outlined here explains the required capabilities to establish an effective CIKR functionality with fusion centers. This document also provides successful processes to synthesize large volumes of CIKR threat, vulnerability, and consequence information into useful, actionable products developed with the ultimate end user in mind.

Protecting critical infrastructure is a shared responsibility by all levels of government and the owners and operators of the nation's critical infrastructure. An effective partnership needs to be fostered among regional and federal CIKR stakeholders to ensure the proper collaboration and a holistic approach to the regional and national security objectives.

Appendix: Background

National Strategy for Information Sharing



The *National Strategy for Information Sharing*, issued in October 2007, calls for a national information sharing capability through the establishment of a national integrated network of fusion centers. Since 2001, the federal government has provided significant grant funding, training, and technical assistance to support the establishment of fusion centers owned and operated by states and major urban areas. The Strategy builds on these efforts and provides a federal government-wide approach to interfacing and collaborating with these fusion centers. Additionally, Appendix I of the Strategy outlines the federal, state, local, and tribal governments' roles and responsibilities for the establishment and continued operations of state and major urban area fusion centers.

Developing the Baseline Capabilities Document

The development of baseline operational standards is called for in the *National Strategy for Information Sharing*[11] and is a key step to reaching one of the Strategy's goals: "Establishing a National Integrated Network of State and Major Urban Area Fusion Centers." Defining these operational standards allows federal, state, and local officials to identify and plan for the resources needed—to include financial, technical assistance, and human support—to achieve the Strategy's goal.

The Strategy recognizes the sovereignty of the state and local governments that own and operate fusion centers. The missions of fusion centers vary based on the environment in which the center operates—some have adopted an "all-crimes" approach; others have also included an "all-hazards"[12] approach. The *National Strategy for Information Sharing* supports and encourages these approaches, while respecting that a fusion center's mission should be defined based on local needs.

In support of the Strategy's goal, the federal government agreed that a "sustained federal partnership with state and major urban area fusion centers is critical to the safety of our nation, and therefore a national priority." While not all fusion centers receive federal grant funding, most fusion centers receive other types of support from the federal government, including technical assistance, training, collocation of federal personnel, and access to federal information and networks. This document will help the federal government better identify how to support fusion centers. The federal government does not intend to use this document for punitive purposes; rather, a common set of capabilities is needed in order for the U.S. Department of Homeland Security, the U.S. Department of Justice, and other federal agencies to ensure they are providing the right types of resources in a consistent and appropriate manner. The capabilities also assist in ensuring that fusion centers have the basic foundational elements for integrating into the national Information Sharing Environment.

To develop the *Baseline Capabilities* document, a group of subject-matter experts representing fusion centers across the country reviewed the *Fusion Center Guidelines* (FCG) and other fusion center-related documents to identify capabilities that should be considered necessary to achieve a baseline operational capability as a fusion center. Additional input was received during subsequent discussions, conference

11 The *National Strategy for Information Sharing* was developed in partnership with Global and other state and local officials, to include fusion center officials.

12 See Glossary of *Baseline Capabilities* document for a definition of all-crimes approach and all-hazards approach.

calls, and meetings. A draft of this document was provided to participants at the 2008 National Fusion Center Conference for comment. Several comments recommended removing references to the private sector; others suggested that support to critical infrastructure and key resources protection activities should not be considered a baseline capability. Accordingly, the document was edited to limit baseline capabilities to ensure that the center:

1. Can disseminate alerts, warnings, and notifications and other relevant analytic reports to the affected critical infrastructure or private sector entity.
2. Has mechanisms in place to receive tips and leads from CIKR entities relevant to the center's mission (terrorism, threats, crime, etc.).

The mechanisms used to pass information to and from these entities will vary, and there is no requirement for the fusion center to be the "owner" of the information sharing mechanism. If a state or major urban area already has a CIKR information sharing capability that is managed by another organization, the fusion center can simply provide information to that entity as needed. The emphasis in the baseline capabilities is ensuring that these matters have been considered and planned for.

The capabilities encourage "consideration" of the private sector's input through an Advisory Board or some other mechanism but do not make it a requirement.

Finally, for fusion centers interested in incorporating the support of CIKR into their fusion process, the *Baseline Capabilities* document refers to this document.

The Recognized Value of CIKR

The Value of Fusion Centers Supporting Critical Infrastructure and Key Resources Protection Activities

Efforts to support the protection of CIKR are an essential component of any overarching homeland security program. In accordance with the *National Infrastructure Protection Plan* (NIPP) risk management framework, as well as the benchmarks and requirements identified in the FY2006 and FY2007 Homeland Security Grant Program (HSGP), state governments are responsible for building and sustaining a statewide/regional CIKR protection program. This program must include the processes necessary to implement the NIPP risk management framework at the state and/or regional level, including urban areas, as a component of the state's overarching homeland security program.

Additionally, the national priorities identified in the *National Preparedness Guidelines* help guide the nation's preparedness efforts to meet its most urgent needs. With the inclusion of NIPP implementation as one of these overarching national priorities, CIKR protection programs form an essential component of state, territorial, local, tribal, and sector-specific homeland security strategies. Achieving that national priority requires meeting a series of objectives that include understanding and sharing information about terrorist threats and other hazards, building security partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. To achieve these efforts, CIKR security partners should have the following:

- Coordinated, risk-based CIKR plans and programs in place addressing known and potential threats.
- Structures and processes that are flexible and adaptable, both to incorporate operational lessons learned and effective practices and also to adapt quickly to a changing threat or incident environment.
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery.
- Access to robust information sharing networks that include relevant intelligence, threat analysis, and real-time incident reporting.[13]

13 *National Preparedness Guidelines*.

These objectives are inherent in the information sharing and intelligence cycle processes that occur within fusion centers on a daily basis, and therefore there is a natural tendency for fusion centers and CIKR protection programs to coordinate and integrate their efforts so that they can more successfully leverage resources and integrate the gathering, analysis, and sharing of CIKR-related information and intelligence with all other threat information, whether criminal, homeland security, or counterterrorism in nature. The coordination and integration of these efforts also support achievement of the Expanded Regional Collaboration and Strengthen Information Sharing and Collaboration national priorities noted in the *National Preparedness Guidelines*.

Therefore, fusion centers are strongly encouraged to consider the integration of state, local, federal, and private sector CIKR protection efforts in their current operational capabilities. **The integration of CIKR capabilities should not be separated from all other ongoing intelligence and information sharing activities; rather, it should be integrated throughout every step of the intelligence process.** This will ensure that CIKR information is appropriately coordinated and integrated with other state, local, federal, and private sector threat information, whether criminal, homeland security, or counterterrorism in nature. The incorporation of CIKR-related information throughout the intelligence processes occurring in the fusion center will provide a more comprehensive understanding of the threat, vulnerabilities, potential consequences of attacks, and the effects of risk-mitigation actions. It will also more successfully allow fusion centers to plan for and support the development of preventative and protective measures to deter, disrupt, and/or mitigate threats.