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

September 2008

Homeland Security

STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT COORDINATING COUNCIL

Office of Infrastructure Protection
National Protection & Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 2008

Critical Infrastructure and Key Resources Partners:

Risk today results from a complex mix of manmade and naturally occurring threats and hazards, including terrorist attacks, hurricanes, earthquakes, floods, power outages, hazardous materials spills, and industrial accidents. Our critical infrastructure and key resources (CIKR) are inherently vulnerable both within and across sectors, due to the nature of their physical, geographical, and virtual interconnections. CIKR protection requires a strategy appropriately balancing resiliency—a traditional American strength in adverse times—with focused, risk-informed prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks we face.

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk analysis and management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security (DHS); Federal Sector-Specific Agencies (SSAs); and other Federal, State, local, tribal, and private sector CIKR partners. The NIPP provides the coordinated approach used to establish national priorities, goals, and requirements for infrastructure protection to ensure that funding and resources are applied effectively.

However, States, regions, and communities have unique concerns arising from the functional and geographical interdependencies and the unique mix of CIKR in their areas. Thus, it is important for State, regional, local, tribal, and territorial CIKR protection and resiliency efforts not only to help implement the NIPP and the associated Sector-Specific Plans (SSPs), but also to support more specific, localized concerns. To assist with this implementation, DHS and the State, Local, Tribal, and Territorial Government Coordinating Council have prepared *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Levels.*

This document outline the attributes, capabilities, needs, and processes that a State or other governmental entity should include in establishing its own CIKR protection function such that it integrates with the NIPP and accomplishes the desired local benefits. It is intended serve as a "why-to" rather than a "how-to" guide. The guide is not intended to be prescriptive or to impose requirements on the States, communities, or other CIKR partners. Rather, it suggests various strategies and approaches, and leaves it to the discretion of each State, region, or locality to determine which approach or combination of approaches, if any, might be suited to their specific needs, operating environments, and risk landscapes.

We ask for your commitment and cooperation in the development and implementation of robust CIKR protection efforts at the State and local level to complement and support our ongoing national efforts.

Robert B. Stephan
Assistant Secretary
Infrastructure Protection

Brigadier General Michael C. McDaniel
Chairman
SLTTGCC

Table of Contents

Preface

States, regions, and communities have unique concerns arising from the functional and geographical interdependencies of critical infrastructure and key resources (CIKR) in their areas, as well as the need to share information across boundaries. Each area also has a unique mix of infrastructure and, as illustrated in their respective Sector-Specific Plans (SSPs), each sector has unique issues and concerns that result in very different approaches to protection. There may be CIKR that are very important to the local economy and the safety and confidence of the population, even if they are not nationally significant. Thus, it is important for State, regional, local, tribal, and territorial CIKR protection and resiliency efforts to help implement the National Infrastructure Protection Plan (NIPP) and the associated SSPs, and also to support more specific, localized concerns. This document helps interpret the requirements of the NIPP at these various non-Federal levels and outlines the attributes, capabilities, needs, and processes that a State or other governmental entity should include in establishing its own CIKR protection function so that it integrates with the NIPP.

CIKR protection is an ongoing process with multiple intersecting elements. The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort that brings together government at all levels, the private sector, nongovernmental organizations, and international CIKR partners. The NIPP addresses infrastructure protection and resiliency in an all-hazards environment. The most effective protective practices and resiliency strategies are often those that offer benefits in the case of terrorist threats as well as natural hazards and man-made failures.

The Department of Homeland Security (DHS) recognizes that implementation of the CIKR protection mission requires the cooperation of, and coordination between, Federal departments and agencies; State, local, tribal, and territorial governments; regional coalitions; private sector owners and operators; and international partners. The NIPP is supported by SSPs that provide further detail on how the CIKR mission of each sector will be carried out. (These documents may be obtained at www.dhs.gov/NIPP or by emailing DHS at NIPP@dhs.gov.)

To align with the NIPP, non-Federal CIKR protection plans and resiliency strategies should explicitly address:

- CIKR protection roles and responsibilities;
- Building partnerships and information sharing;
- Implementing the NIPP Risk Analysis/Management Framework;
- Developing procedures for data use and protection;
- Leveraging ongoing sector-based activities for CIKR protection and resiliency; and
- Integrating Federal and sector CIKR protection activities.

This document speaks to all of these points, describing their importance and purpose. It is intended to serve as a “why-to” rather than a “how-to” guide. This document is written for Homeland Security Advisors (HSAs), State Administrative Agencies (SAAs), Urban Area Working Groups (UAWGs), regional groups and coalitions, and other State and local agency leads with responsibilities that include aspects of homeland security. The roles and responsibilities of these CIKR partners differ by State and region, depending on whether the area of concern crosses State or international borders, the authorities supporting each agency, and the way in which homeland security is addressed, managed, and funded in each area. In addition, much of the information presented will be useful to those responsible for homeland

security practices and initiatives at the territorial, tribal, or local level. Application at these levels also will vary based on the many different forms of government (town, city, county, township, tribe, etc.), the local delegations of authority, budget constraints, and the numbers and types of CIKR within any given community.

This document is not intended to be prescriptive or to impose requirements on the States, communities, or other CIKR partners. Rather, it suggests various strategies and approaches, and leaves it to the discretion of each State, region, or locality to determine which approach or combination of approaches, if any, might be suited to their specific needs, operating environments, and risk landscapes. Appendices to this document and other documents, such as the Archangel Guidebook (Protecting Critical Infrastructure & Key Resources (CI/KR): A Guidebook for States, Regions, Local, and Tribal Communities for Implementing CI/KR Protection Programs), provide guidance on how to carry out each of these activities.

Executive Summary

This document serves as a high-level guide for Homeland Security Advisors (HSAs), State Administrative Agencies (SAAs), Urban Area Working Groups (UAWGs), regional groups and coalitions, and other agency leads with responsibilities that include aspects of infrastructure protection. The roles and responsibilities of these CIKR partners differ by State and region, depending on whether the area of concern crosses State or international borders, the authorities supporting each agency, and the way in which homeland security and infrastructure protection are addressed, managed, and funded in each area. In addition, much of the information presented will be useful to those responsible for homeland security practices and initiatives at the local, tribal, or territorial level. Application at these levels also will vary based on the many different forms of government (town, city, county, township, tribe, etc.), the local delegations of authority, budget constraints, and the numbers and types of critical infrastructure and key resources (CIKR) within any given community.

This document is not intended to be prescriptive or to impose requirements on the States, communities, or other CIKR partners. Rather, it suggests various strategies and approaches, and leaves it to the discretion of each jurisdiction to determine which approach or combination of approaches, if any, might be suited to their specific needs, operating environments, and risk landscapes.

1. Introduction

The goal of the National Infrastructure Protection Plan (NIPP) is to:

> *Build a safer, more secure, and more resilient America by enhancing protection of the Nation's critical infrastructure and key resources (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 sets forth a comprehensive risk analysis and management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security (DHS); Federal Sector-Specific Agencies (SSAs); and other Federal, State, regional, local, tribal, territorial, and private sector CIKR partners. The NIPP provides the coordinated approach used to establish national priorities, goals, and requirements for infrastructure protection to ensure that funding and resources are applied effectively. The NIPP is supported by a Sector-Specific Plan (SSP) for each of the CIKR sectors, tailoring the national approach to the specific concerns and risk landscape of individual sectors.

Non-Federal CIKR protection programs are essential to implementing the principles and programmatic activities outlined in the NIPP. State and local officials and regional organizations play an important role in leading or supporting their respective CIKR protection programs and in the overall implementation of the NIPP. They provide jurisdictional focus, facilitate bottom-up information sharing and collaboration, and enable cross-sector coordination by applying the NIPP risk management framework across the vertically organized CIKR sectors within their communities.

To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership framework and information-sharing network. The

coordination mechanisms establish linkages among CIKR protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels as well as between public and private sector CIKR partners. In addition to direct coordination between CIKR partners, the structures described in section 1.2 provide a national framework that fosters relationships and facilitates coordination within and across CIKR sectors.

The NIPP sets out a number of responsibilities for State, local, tribal, and territorial (SLTT) governments and regional organizations; many relate to developing and utilizing strong partnerships. These responsibilities are summarized in section 1.3 and interpreted throughout the rest of this document. Collectively, these efforts create a protective envelope for our Nation's CIKR. These non-Federal efforts are the ones that are most visible and tangible to many of the owners and operators—as well as to the public in general.

2. Planning for CIKR Protection

State homeland security strategies align with and support the priorities established in the National Preparedness Guidelines (*Guidelines)*. With the inclusion of NIPP implementation as one of these national priorities, CIKR protection plans and programs form an essential component of State (and local) homeland security strategies, particularly with regard to establishing funding priorities and informing security investment decisions.

To permit effective NIPP implementation and performance measurement at each jurisdictional level, State CIKR protection plans and programs should reference all core elements of the NIPP framework, including key cross-jurisdictional security and information-sharing linkages, as well as specific CIKR protective programs focused on risk management. These plans and programs play a primary role in the identification and protection of CIKR locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CIKR of national-level criticality within the jurisdiction or area.

Chapter 2 also describes the complementary relationship of the NIPP and the National Response Framework, as well as some of the applicable grant programs.

3. Information Sharing and Protection

The primary objective of the NIPP approach to information sharing is to enhance situational awareness and maximize the ability of government and private sector CIKR partners at all levels to assess risks and execute risk mitigation programs and activities. States and other groups can collaborate with DHS, SSAs, other State and local agencies, and private sector CIKR partners to encourage the development of appropriate information-sharing and analysis processes and mechanisms to support these processes. Including CIKR protection capabilities in a fusion center will assist State, regional, and local CIKR partners in mitigating and responding to terrorist threats as well as man-made or natural hazards.

Effective CIKR information sharing relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end-user's homeland security responsibilities and "need to know" the information in question. Whether the sharing is "top-down" (by partners working with national-level information such as system-wide aggregate data or the results of emergent threat analysis by the Intelligence Community) or "bottom-up" (by field personnel or facility operators sharing

detailed and location-specific information), the network approach places shared responsibility on all CIKR partners to adhere to applicable information-sharing protocols and practices.

4. Using the Risk Management Framework to Develop a Plan

The risk management framework set out in the NIPP and tailored in each of the SSPs also serves as a constructive model to build State, regional, and community CIKR protection plans and resiliency strategies. Following the framework helps ensure that all the plans are compatible and that CIKR partners can communicate clearly about the different plans. Chapter 4 describes the intent and suggested content (high level) of each section of a State, regional, or community CIKR protection plan, including:

- Setting Goals, Objectives, and Criteria
- Identifying Assets, Systems, and Networks
- Assessing Risks
- Prioritizing Infrastructure
- Developing and Implementing Protective Programs and Resiliency Strategies
- Measuring Progress

5. Cybersecurity Considerations

Responsibility for cybersecurity is shared across public and private sector entities, including State and local governments, and individual citizens. DHS' National Cybersecurity Division (NCSD), the Nation's focal point for cybersecurity, is committed to working with entities at various jurisdictional levels to enhance the Nation's cybersecurity posture and offers a variety of cybersecurity resources and technical assistance to help SLTT governments address cybersecurity as part of national and State CIKR protection efforts. As SLTT government entities establish and enhance their own CIKR protection function, they should consider the following strategies and approaches related to cybersecurity.

- Raise awareness of cyber risk and the importance of implementing cybersecurity practices;
- Develop and implement cybersecurity policies, plans, and procedures;
- Build and maintain relationships with CIKR partners;
- Share and obtain information through established policy and operational mechanisms;
- Identify cyber assets, systems, networks, and functions;
- Implement a risk management program;
- Develop and enhance cybersecurity operational capabilities; and
- Exercise and test cybersecurity policies, plans, and procedures and operational capabilities.

6. Coordinating CIKR Protection R&D Efforts

HSPD-7 establishes an annual requirement for a national R&D plan for CIKR protection. The National Critical Infrastructure Protection (NCIP) R&D Plan is the result of a collaborative process undertaken by the Federal CIKR protection community as well as CIKR partners from the sectors. This process involves collecting information on R&D requirements from a broad range of CIKR partners, and then prioritizing those requirements based on risk. States and localities can contribute to the requirements and prioritization process by working with the SLTTGCC as well as the relevant individual sectors. They should also work with DHS, the

SSAs, local universities and research organizations, as well as private companies to identify research that may be underway in their jurisdictions (or elsewhere) to fill gaps in protective programs. Certain States may also have their own research programs, particularly in sectors like Agriculture and Food or Water.

7. Managing CIKR Protection Programs and Activities

Each State, region, or locality is likely to manage its homeland security responsibilities differently. CIKR protection activities may be centralized in one agency (e.g., Homeland Security, Public Safety, or Emergency Management) or spread across different agencies (including the Departments of Public Health, Environmental Protection, and Agriculture as well as the Public Utilities Commission), or entirely ad hoc. Therefore, it is important that the management processes the State or locality has established and/or will establish to support its responsibilities under the NIPP are defined and specific as to how the State or locality will ensure those responsibilities are satisfied. The roles and responsibilities of different parties should be defined, along with coordination mechanisms. This is potentially even more complex when multiple States and/or combinations of private sector and government CIKR partners are involved in regional frameworks.

The successful implementation of the NIPP and the SSPs, as well as State, regional, or local CIKR protection plans, relies on building and maintaining individual and organizational CIKR protection expertise. Training and education in a variety of areas are necessary to achieve and sustain this level of expertise. In addition, effective implementation of the plan and program will require specific, task-oriented implementation plans that have broad buy-in and allow CIKR partners to accomplish critical activities on an appropriate and defined time scale.

1. Introduction

1.1 Background – The NIPP and the SSPs

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk analysis and management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security (DHS); Federal Sector-Specific Agencies (SSAs); and other Federal, State, local, tribal, and private sector CIKR partners. The NIPP provides the coordinated approach used to establish national priorities, goals, and requirements for infrastructure protection to ensure that funding and resources are applied effectively.

The goal of the NIPP is to:

> *Build a safer, more secure, and more resilient America by enhancing protection of the Nation's critical infrastructure and key resources (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.*

As noted in the goal, the NIPP addresses infrastructure protection and resiliency in an all-hazards environment. The most effective protective practices and programs are often those that offer benefits in the case of terrorist threats as well as natural hazards and man-made failures.

CIKR includes assets, systems, and networks, whether physical or virtual, so vital that their failure or destruction would have a debilitating impact on security, continuity of government, continuity of operations, public health and safety, public confidence, or any combination of these effects.

Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident (see figure). Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, implementing cybersecurity measures, and conducting training, exercises, and business continuity planning, among various others.

Achieving the NIPP goal requires meeting a series of objectives that include understanding and sharing information about terrorist threats and other hazards, building CIKR partnerships,

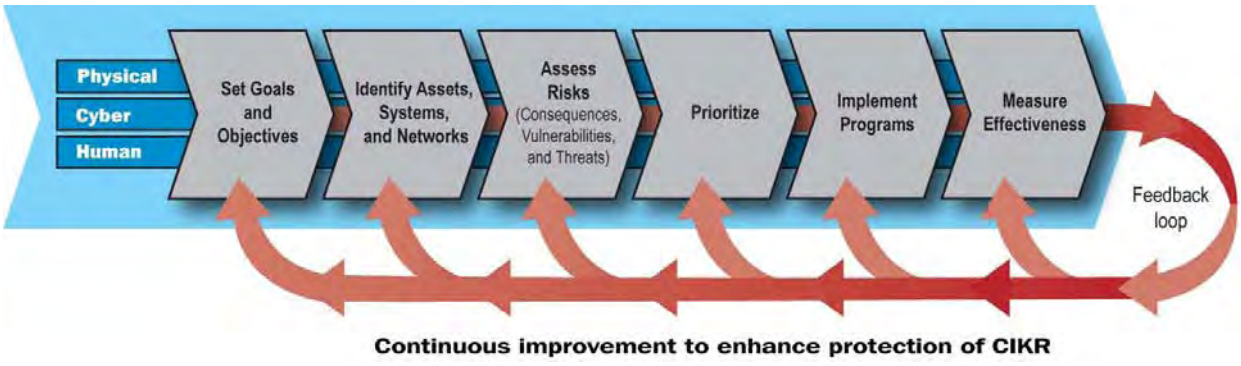
implementing a long-term risk management program, and maximizing the efficient use of resources. CIKR partners should have the following plans and processes in place to achieve the NIPP goal:

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

These plans and processes apply to State, regional, and other community organizations, just as they do to SSAs and CIKR owners and operators. Geographically based CIKR protection programs play an important role in ensuring the long-term success of CIKR protection efforts as they involve direct contact with infrastructure owners and operators on a sustained basis.

The cornerstone of the NIPP is the Risk Management Framework, as depicted below. This Framework establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive and systematic assessment of risks to assets, systems, networks, and functions of potential interest. The Risk Management Framework has six main steps: 1) set goals and objectives; 2) identify assets, systems, and networks; 3) assess risk based on consequences, vulnerabilities and threats; 4) establish priorities based on risk results; 5) develop and implement protective programs and resiliency strategies; and 6) measure effectiveness. This framework results in the identification and development of prioritized protective measures and resiliency strategies, and helps enhance critical infrastructure protection and resiliency through continuous improvements over time.

Risk Management Framework



Federal SSAs are responsible for implementing the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CIKR sectors designated in Homeland Security Presidential Directive 7 (HSPD-7). The SSPs complement the NIPP and detail the application of the NIPP risk management framework specific to each of the CIKR sectors. The SSPs were developed by the designated SSAs (see table) in close collaboration with sector CIKR partners and establish sector goals; tailor approaches for identifying,

assessing, and prioritizing assets, systems, and networks; describe sector approaches to protective programs; and discuss the use of metrics for continuous improvement and the determination of overall progress. SSAs have a key role, along with their Sector and Government Coordinating Councils, in providing leadership and coordination for a single sector. They provide Federal level guidance and support and work across States, regions, and communities, but with a focus on their particular sector.

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture[1] Department of Health and Human Services[2]	Agriculture and Food
Department of Defense[3]	Defense Industrial Base
Department of Energy	Energy[4]
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security *Office of Infrastructure Protection*	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration, United States Coast Guard[5]	Transportation Systems[6]
Immigration and Customs Enforcement, Federal Protective Service	Government Facilities[7]

1 The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).
2 The Department of Health and Human Services, Food and Drug Administration is responsible for food other than meat, poultry, and egg products.
3 Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
4 The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for nuclear power facilities.
5 The U.S. Coast Guard is the SSA for the maritime transportation mode.
6 As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.
7 The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

Non-Federal CIKR protection programs are essential to implementing the principles and programmatic activities outlined in the NIPP. State and other non-Federal leaders, including regional boards or coalitions, can provide the organizational structures that ensure coordination between and among all levels of government and the private sector, such as State-level coordinating councils. These councils can then be responsible for leading or coordinating efforts to identify CIKR, conduct risk assessments, prioritize the results of these assessments, examine interdependencies, and develop and implement protective programs and resiliency strategies. States, regions, and communities are encouraged to focus their efforts in ways that leverage Federal resources and address each sector's requirements in their particular areas.

State and local officials play an important role in leading or supporting their respective CIKR protection programs and in the overall implementation of the NIPP. They provide jurisdictional focus, facilitate bottom-up information sharing and collaboration, and enable cross-sector coordination by applying the NIPP Risk Management Framework across the vertically organized CIKR sectors within their communities. Fundamentally, State and local organizations should implement their homeland security missions to ensure public safety and welfare and provide for the continued delivery and operation of essential services to their constituencies.

Regional organizations, whether interstate or intrastate, vary widely in terms of mission, composition, and functionality. Regardless of the variations, these organizations provide structures at the strategic and/or operational levels that help to address cross-sector CIKR planning, interdependencies, and program implementation. They also may provide enhanced coordination between jurisdictions within a State where CIKR cross multiple jurisdictions, and help sectors coordinate with multiple States that rely on a common set of CIKR. In a regional context, the NIPP risk management framework and information-sharing processes can be applied through the development of a regional partnership model or the use of existing regional coordinating structures.

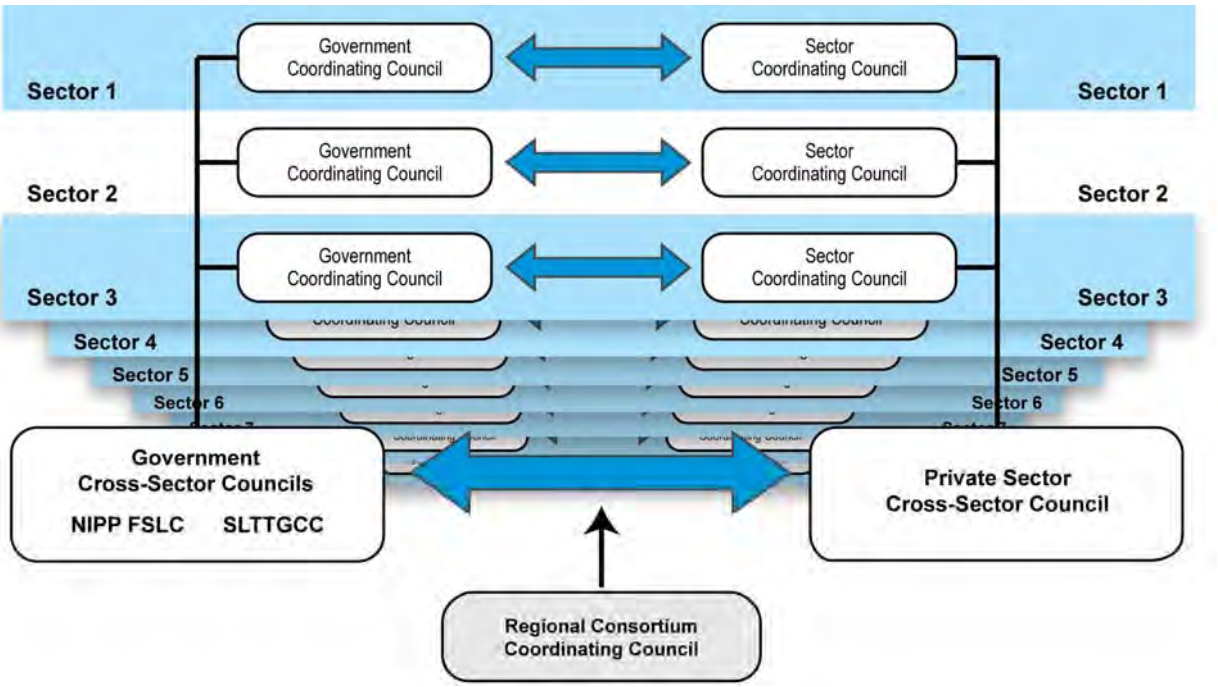
1.2 Sector Partnership Model

To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership framework and information-sharing network. The coordination mechanisms establish linkages among CIKR protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels as well as between public and private sector CIKR partners. In addition to direct coordination between CIKR partners, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CIKR sectors.

- **Sector Partnership Coordination.** The CIKR Private Sector Cross-Sector Council, the Government Cross-Sector Council (made up of two subcouncils: the NIPP Federal Senior Leadership Council and the State, Local, Tribal, and Territorial Government Coordinating Council), the Regional Consortium Coordinating Council, and individual Sector Coordinating Councils and Government Coordinating Councils create a structure through which representative groups from government and the private sector can collaborate and develop consensus approaches to CIKR protection.
- **Sector Coordinating Councils.** The sector partnership model encourages CIKR owners and operators to create or identify an SCC as the principal private sector entity for coordinating with the government on a wide range of CIKR protection activities and issues. Specific membership will vary by sector, reflecting each sector's unique

composition; however, membership should be representative of a broad base of owners, operators, associations, and other entities—large and small—within a sector.

- **Government Coordinating Councils.** A GCC is formed as the government counterpart to the SCC to enable interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (Federal, State, local, tribal, and territorial) as appropriate to the security landscape of each individual sector.



- **Regional Consortium Coordinating Council (RCCC).** The RCCC brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among CIKR partners within and across geographical areas and sectors.
- **International Coordination.** The United States-Canada-Mexico Security and Prosperity Partnership, the North Atlantic Treaty Organization's Senior Civil Emergency Planning Committee, certain government councils such as the Committee on Foreign Investment in the United States, and consensus-based nongovernmental or public-private organizations enable a range of CIKR protection coordination activities associated with established international agreements.
- **Critical Infrastructure Partnership Advisory Council (CIPAC).** The CIPAC directly supports the sector partnership model by providing a legal framework for members of the SCCs and GCCs to engage in joint CIKR protection-related activities. The CIPAC serves as a forum for government and private sector CIKR partners to engage in a broad spectrum of activities including: planning, coordination, implementation, and operational issues; implementation of security programs; operational activities related to CIKR protection including incident response, recovery, and reconstitution; and development and support of national plans, including the NIPP and Sector-Specific Plans.

1.3 Roles and Responsibilities

The NIPP sets out a number of responsibilities for State, local, tribal, and territorial governments and regional organizations. These are summarized below and interpreted throughout the rest of this document. Collectively, these efforts create a protective envelope for our Nation's CIKR. These non-Federal efforts are the ones that are most visible and tangible to many of the owners and operators—as well as to the public in general. There also may be State-level coordinating councils that are very engaged with owners and operators.

State/Territorial

State (and territorial, where applicable) governments should establish CIKR partnerships, facilitate coordinated information sharing, and enable planning and preparedness for CIKR protection within their jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities; capacities; and resources among local jurisdictions, across sectors, and between regional entities. States and territories also act as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public and private sector CIKR partners at lower jurisdictional levels. States receive CIKR information from the Federal Government to support national and State CIKR protection and resiliency programs.

State and territorial governments should develop and implement State or territory-wide CIKR protection programs that reflect the full range of NIPP-related activities. State/territorial programs should address all relevant aspects of CIKR protection, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional CIKR protection efforts should be integrated into the over-arching homeland security program framework at the State or territory level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive. CIKR protection at the State/territory level cuts across all sectors present within the State/territory and should support national, State, and local priorities. The program also should explicitly address unique geographical issues, including trans-border concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific CIKR protection-related activities at the State/territorial level include:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local jurisdictions and regional partners;
- Developing a consistent approach to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant stakeholders within their jurisdictions;
- Identifying, implementing, and monitoring a risk management plan and taking corrective actions as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the capabilities of State and local jurisdictions and private entities resident within them;

- Facilitating the exchange of security information, including threat assessments and other analyses, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in and coordinating with the existing NIPP sector partnership model, including Government Coordinating Councils (GCCs) like the State, Local, Tribal, and Territorial GCC; Sector Coordinating Councils (SCCs); and other CIKR governance efforts and SSP planning efforts relevant to the given jurisdiction to include the State or jurisdiction's customized version of a sector partnership model, such as combined GCCs/SCCs which demand less support [Note: it is not necessary to create parallel councils at the State level, although this may be desired in some States or regions];
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with relevant plans and strategies;
- Sharing information on CIKR deemed critical from national, State, regional, local, tribal, and/or territorial perspectives to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for increases in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System (HSAS);
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR protection context;
- Providing response and protection where there are gaps and local entities lack resources to address these gaps;
- Identifying and communicating State and territorial needs or requirements for CIKR-related R&D to DHS; and
- Providing information, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and CIKR-related funding projections.

Regional

Regional CIKR partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on homeland security preparedness, protection, response, and recovery within or serving the population of a defined geographical area. Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding CIKR protection.

CIKR partners leading or participating in regional initiatives are encouraged to capitalize on the larger area- and sector-specific expertise and relationships to:

- Promote collaboration among CIKR partners in implementing NIPP-related CIKR risk assessment and protection activities;
- Facilitate education and awareness of CIKR protection efforts occurring within their geographical areas;

- Coordinate regional exercise and training programs, including a focus on CIKR protection collaboration across jurisdictional and sector boundaries;
- Support threat-initiated and ongoing operations-based activities to enhance protection and preparedness, as well as to support mitigation, response, and recovery;
- Work with State, local, tribal, territorial, and international governments and the private sector, as appropriate, to evaluate regional and cross-sector CIKR interdependencies, including cyber considerations;
- Conduct appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional CIKR protection activities and enhanced response to emergencies;
- Facilitate information sharing and data collection between and among regional initiative members and external partners;
- Share information on progress and CIKR protection requirements with DHS, the SSAs, the States, and other CIKR partners, as appropriate; and
- Participate in the NIPP sector partnership model, as appropriate.

Local

Local governments represent the front lines for homeland security and, more specifically, for CIKR protection and implementation of the NIPP risk management framework and sector partnership model. They provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local government entities own and operate CIKR such as water, stormwater, and electric utilities. Most disruptions or malevolent acts that impact CIKR begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network. Local governments drive emergency preparedness, lead and support NIPP and SSP implementation activities, and encourage the participation of local CIKR partners, including government agencies, owners and operators, and private citizens in the communities they serve.

CIKR protection focus at the local level includes, but is not limited to:

- Acting as a focal point for and promoting the coordination of protective and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a consistent approach at the local level to CIKR identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant CIKR partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Facilitating the exchange of security information, including threat assessments, attack indications and warnings, and advisories, among CIKR partners within the jurisdiction;
- Participating in the NIPP sector partnership model, including GCCs, SCCs, SLTTGCC, and other CIKR governance efforts and SSP planning efforts relevant to the given jurisdiction, through direct participation, coordination, or establishment of local coordinating councils as appropriate;

- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the CIKR protection mission in accordance with those plans and strategies in effect at the national, State, and local levels;
- Sharing information with CIKR partners, as appropriate through HSIN and other channels, on CIKR deemed critical from the local perspective to enable prioritized protection and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for step-ups in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the HSAS;
- Integrating CIKR protection into existing plans, such as hazard mitigation plans, emergency operations plans, and contingency plans;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the CIKR protection context; and
- Conducting CIKR protection public awareness activities.

Tribal

Tribal government roles and responsibilities regarding CIKR protection generally mirror those of State and local governments as detailed above. Tribal governments are accountable for the public health, welfare, and safety of tribal members, as well as the protection of CIKR and continuity of essential services under their jurisdiction. Under the NIPP partnership model, tribal governments ensure close coordination with Federal, State, local, and international counterparts to achieve synergy in the implementation of the NIPP and SSP frameworks within their jurisdictions. This is particularly important in the context of information sharing, risk analysis and management, awareness, preparedness planning, protective program investments and initiatives, and resource allocation.

2. Planning for CIKR Protection

DHS required that each State develop a homeland security strategy with established goals and objectives for its homeland security program that included CIKR protection as a core element. State Administrative Agencies (SAAs) for homeland security funding use these strategies to prioritize statewide resource needs in support of these efforts. The SAA and infrastructure protection specialists at the State and regional level also work with DHS to identify:

- Priorities and annual goals for CIKR protection;
- State-specific requirements for CIKR protection activities and programs, based on risk and need;
- Mechanisms for coordinated planning and information sharing with government and private sector CIKR partners;
- Unfunded CIKR protection initiatives or requirements that should be considered for funding using Federal grants (described in further detail below); and
- Other funding sources utilized to implement the NIPP and address identified priorities and annual goals.

For consideration in the deliberations related to CIKR protection as part of the Federal budget cycle, information on statewide CIKR needs must be reported to DHS by the date specified in the appropriate annual planning guidance. DHS includes information such as model reports or report templates with the planning guidance to support the States' reporting efforts. The homeland security strategies also align with and support the priorities established in the National Preparedness Guidelines (*Guidelines)*. With the inclusion of NIPP implementation as one of these national priorities, CIKR protection plans and programs form an essential component of State (and local) homeland security strategies, particularly with regard to establishing funding priorities and informing security investment decisions.

To permit effective NIPP implementation and performance measurement at each jurisdictional level, State CIKR protection plans and programs should reference all core elements of the NIPP framework, including key cross-jurisdictional security and information-sharing linkages, as well as specific CIKR protective programs focused on risk management. These plans and programs play a primary role in the identification and protection of CIKR locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the protection of CIKR of national-level criticality within the jurisdiction or area.

Establishing CIKR protection plans and programs, particularly those that are cross-jurisdictional and multi-sector, will help States, territories, regional organizations, and tribal and local communities with both their implementation of the NIPP and their efforts in support of the national priority under the *Guidelines* that addresses the NIPP. In addition, CIKR protection plans and programs will also support other initiatives identified in the *Guidelines*, the Target Capabilities List (TCL), and Homeland Security Grant Program (HSGP) guidance. Potential benefits include expanded regional collaboration; cross-jurisdictional resource sharing; strengthened information sharing with local owners and operators; greater engagement of intelligence agencies and fusion centers; and strengthened counterterrorism and all-hazards planning at the State and regional level, as well as by owners and operators.

Current Cross-Jurisdictional, Multi-Sector Planning and Implementation Efforts

The ***Lower Manhattan Security Initiative*** entails the implementation of a comprehensive security plan for lower Manhattan. It includes assessments of clusters of high-risk assets and other measures to enhance critical infrastructure protection in this densely populated area. In 2008, DHS and local CIKR partners planned, coordinated, and completed assessments to be used in the Buffer Zone Plans for this initiative.

CIKR partners also conducted a high-risk cluster assessment pilot on 32 assets in the ***District of Columbia Metroplex Initiative*** and completed cross-sector, multi-asset Buffer Zone Plans as part of this initiative.

The Comprehensive Review (CR) of the ***California Water System***, a multi-jurisdictional and geographically diverse system, involved over 40 critical assets and comprehensive National Infrastructure Simulation and Analysis Center modeling. This CR includes Buffer Zone Plans supporting BZPP grant funds to local law enforcement.

2.1 CIKR Protection and Grants

In addition to providing resources and guidance to achieve the *Guidelines*, the HSGP and other Federal grant programs play an important role in coordinating the national effort to strengthen homeland security and preparedness. The HSGP promotes the implementation of objectives addressed in a series of post-9/11 laws, strategy documents, plans, and HSPDs and defines investment strategies aligned with the National Priorities. Currently, establishing programs to enhance the protection of CIKR is a focus area for certain Federal grant programs; therefore, CIKR protection programs help implement both the Federal investment strategy identified by the *Guidelines* and the HSGP funding priorities.

For purposes of the NIPP, available Federal grants can be grouped into two broad categories: (1) overarching homeland security programs that provide funding for a broad set of activities in support of homeland security mission areas and the national priorities outlined in the *Guidelines*, and (2) targeted infrastructure protection programs for specific CIKR-related protection initiatives and programs within identified jurisdictions. States should leverage the range of available resources, including those from Federal, State, local, tribal, and territorial sources, as appropriate, in support of the protection activities needed to reduce vulnerabilities and close identified capability gaps related to CIKR within their jurisdictions. These grant programs are described further in Appendix A.

2.2 The NIPP and the NRF -- *Complementary Efforts*

The *National Response Framework (NRF)* establishes a comprehensive, national, all-hazards approach to domestic incident response. The framework presents an overview of key response principles, roles, and structures that guide the national response. It describes how communities, States, the Federal Government, and private sector and nongovernmental partners apply these principles for a coordinated, effective national response. It also describes special circumstances where the Federal Government exercises a larger role, including incidents where Federal interests are involved and catastrophic incidents where a State would require significant support. Its real value, however, is in how these elements come together and are implemented by first responders, decision makers, and supporting entities to provide a unified national response.

The framework is written for senior elected and appointed leaders, such as Federal agency heads, State Governors, tribal leaders, mayors, or city managers – those who have a

responsibility to provide for effective incident management. At the same time, it informs emergency management practitioners, explaining the operating structures and tools used routinely by first responders and emergency managers at all levels of government.

In terms of incident management, the NIPP establishes the overall risk-based approach that defines the Nation's CIKR steady-state protective posture, while the NRF and National Incident Management System (NIMS) provide the overarching mechanisms and protocols required for effective and efficient domestic incident management. The NIPP risk management framework, information-sharing network, and sector partnership model provide vital functions that, in turn, inform and enable incident management decisions and activities.

The Critical Infrastructure and Key Resources Support Annex (released in January 2008) is an important part of the NRF. This annex describes policies, roles and responsibilities, and the concept of operations for assessing, prioritizing, protecting, and restoring CIKR of the United States and its territories and possessions during actual or potential domestic incidents. It serves as the bridge between the steady-state CIKR protection activities of the NIPP and the SSPs and actual incident response. The annex details processes to ensure coordination and integration of CIKR-related activities among a wide array of public and private incident managers and CIKR partners within immediate incident areas as well as at the regional and national levels. You may obtain the annex and the NRF at http://www.fema.gov/emergency/nrf/.

2.3 Working with CIKR Partners

In order to ensure that the State and local perspective was included in the partnership model and to network the private sector with all levels of government, DHS enabled and facilitated the formation of the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The SLTTGCC functions as a forum for State, local, tribal, and territorial government representatives across functional disciplines to engage with the Federal Government and CIKR owners and operators within the partnership model, to achieve the CIKR protection mission. The SLTTGCC allows State, local, tribal, and territorial governments to actively coordinate across their jurisdictions and with the Federal Government on CIKR protection guidance, strategies, and programs. Additionally, the SLTTGCC is the second subcouncil of the Government Cross-Sector Council, as prescribed in the NIPP, which provides the forum to address cross-sector issues and interdependencies between the GCCs.

SLTTGCC accomplishments to date include:

- **Implementation of Representation to the Government Coordinating Councils.** The SLTTGCC reached out across the sectors to initiate membership involvement within each sector GCC. The SLTTGCC has also examined which additional Federal, State, and local representatives could be added to its membership.
- **Development of HSIN-SLTTGCC.** The Homeland Security Information Network-SLTTGCC (HSIN-SLTTGCC) site is functional, and each working group has its own portal. A working group, the Communication and Coordination Working Group (CCWG), was formed to address the expansion of information and services provided with HSIN as a primary portal.
- **Review of Sector-Specific Plans.** The SLTTGCC, through its Policy and Planning Working Group, reviewed each SSP and provided recommendations for its improvement.
- **Development of Baseline Capabilities for CIKR Functions in Fusion Centers.** The SLTTGCC, through its Information Sharing and Collaboration Working Group, identified

the minimum functions necessary to adequately integrate CIKR intelligence functions into State and UASI fusion centers.

- **Identification of Baseline Characteristics for Regional Partners.** The SLTTGCC has developed a set of baseline characteristics to aid SLTT entities in identifying regional CIKR organizational partners.
- **Participation in the Development of the 2008 National CIKR Annual Report.** The Policy and Planning Working Group developed the SLTTGCC Appendix to the National Annual Report.

The SLTTGCC is currently engaged in a variety of initiatives to advance CIKR protection, vulnerability reduction, and consequence mitigation. Examples of these initiatives include:

- The SLTTGCC's Information Sharing and Collaboration Working Group is currently collaborating with DHS, the National Fusion Center Coordinating Group, and the Criminal Intelligence Coordinating Council on the integration of critical infrastructure and key resource intelligence and analysis capabilities into all fusion centers nationwide.
- The Policy and Planning and Information Sharing and Collaboration Working Groups are currently developing an implementation guide that provides guidance to SLTT entities on how to engage existing organizations, or initiate new organizations where coordination across sectors, disciplines, and jurisdictions is necessary for CIKR protection and resiliency.
- The C/ACAMS Working Group is working to further develop the Constellation/Automated Critical Asset Management System tool and to promote enhanced efforts to protect critical infrastructure at all levels of government. The working group is continually engaged with DHS/IP's Infrastructure Information Collection Division (IICD) to upgrade the C/ACAMS systems and functions, improve system responsiveness, increase user friendliness, and improve on-the-ground inventorying processes.
- The Chemical-terrorism Vulnerability Information Working Group has engaged with the Infrastructure Security Compliance Division (ISCD) regarding the various elements of the Chemical Facilities Anti-Terrorism Standards (CFATS). Central to this is the variety of comments and recommendations to the ISCD on the promulgation of a CVI sharing process, in which State and local officials with a need to know can access data on risks of selected facilities that manufacture, store or otherwise use security-sensitive chemicals.

The SLTTGCC strives to achieve geographical diversity and broad discipline representation through its membership. Members must meet the following criteria:

- A State, local, or tribal homeland security director or equivalent who has both programmatic planning and operational responsibilities related to CIKR protection.
- Accountable for the development, improvement, and maintenance of critical infrastructure protection policies or programs at the State, local, tribal, or territorial level.
- Recognized among his/her peers as a leader, with relevant knowledge and experience.
- Committed to acting as a national representative for their stakeholders and willing to be actively engaged in promoting and facilitating the implementation of communication and coordination among their stakeholders on CIKR protection policies, strategies, and programs.

Currently the SLTTGCC consists of a diverse geographical membership stretching from Alaska to the Virgin Islands. The SLTTGCC draws its members from twelve States, six cities, three counties, three tribes, and two regional governments. Members come from a diverse professional background; presently members are state homeland security advisors, city managers, law enforcement, emergency services, and public health officials. The council represents jurisdictions that are well distributed across rural, urban, and suburban populations.

States and communities seeking additional information, membership, or the opportunity to review and comment on various SLTTGCC products should email SLTTGCC@dhs.gov.

State-Level Coordinating Councils

A number of States have found it beneficial to emulate the Sector and Government Coordinating Council structure at the State or regional level—this can also be done at a local level, but such a level of formality will not generally be needed. Such councils provide additional opportunities for public and private sector CIKR partners to work together to develop and implement protective plans and resiliency strategies, to contribute to annual reporting processes, and to identify R&D and training requirements. The particular coordinating councils that you establish should depend on the CIKR present in your jurisdiction or geographical area—and the interests of your CIKR partners.

Working with CIKR Partners

When working with any CIKR partner, from the private sector to other State agencies, anticipate the question, "What's in it for me?" Be ready to respond with the results of research or your existing knowledge on motivating factors and leveraging points, such as protection of future profits, safety of employees, or ability to carry out critical missions.

Consider pointing out that your plans and related activities can assist in:

- Providing owners and operators with information on threats to CIKR that is as timely, analytical, and accurate as possible;
- Ensuring industry is engaged as early as possible in the development and enhancement of risk management activities, approaches, and actions;
- Ensuring industry is engaged as early as possible in the development and revision of CIKR protection plans and in other CIKR protection initiatives;
- Creating an environment that helps to establish incentives and encourages companies to voluntarily adopt sound security practices; and
- Understanding the interdependencies between CIKR sectors and enhancing business continuity planning.

3. Information Sharing and Protection

3.1 Information Sharing

The primary objective of the NIPP approach to information sharing is to enhance situational awareness and maximize the ability of government and private sector CIKR partners at all levels to assess risks and execute risk mitigation programs and activities. States and other groups can collaborate with DHS, SSAs, other State and local agencies, and private sector CIKR partners to encourage the development of appropriate information sharing and analysis processes and mechanisms to support these processes.

When owners and operators are provided with a comprehensive picture of threats or hazards to CIKR and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped with an understanding of private-sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly. States and localities often serve as one of the bridges between all levels of government and owners and operators. Thus, it is important to define and describe information-sharing mechanisms that are used by the State, region, or locality and the processes, programs, and tools that are in place to ensure protection of CIKR information that is collected.

Homeland Security Information Network (HSIN)
HSIN is a robust and significant information-sharing system that supports NIPP-related steady-state CIKR protection and NRF-related incident management activities, as well as serving the information-sharing processes that form the bridge between these two homeland security missions. The linkage between the nodes results in a dynamic view of the strategic risk and evolving incident landscape. HSIN functions as one of a number of mechanisms that enable DHS, SSAs, States/regions/territories/localities, and other partners to share information. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness of all CIKR partners in an all-hazards environment. HSIN network architecture design is informed by experience gained by DoD and other Federal agencies in developing networks to support similar missions. It supports a secure common operating picture for all CIKR partner command or watch centers, including those of supporting emergency management and public health activities.

The HSIN is composed of multiple, non-hierarchical communities of interest (COIs) that offer partners the means to share information based on secure access. COIs provide virtual areas where groups of participants with common concerns, such as law enforcement, counterterrorism, critical infrastructure, emergency management, intelligence, international, and other topics, can share information. This structure allows government and industry partners to engage in collaborative exchanges, based on specific information requirements, mission emphasis, or interest level.

DHS encourages each State, region, or locality to determine the information-sharing mechanisms that best meet its needs and those of its owners and operators. The opportunity exists to implement a tailored information-sharing solution that may include a combination of tools such as the Homeland Security Information Network (HSIN) and other new and/or existing mechanisms offered by fusion centers, trade associations, Information Sharing and Analysis Centers (ISACs), security organizations, and industry-wide or corporate operations centers.

Owners and operators have the greatest understanding of their own physical and cyber assets, systems, and networks. States, regions, or localities should work with owners and operators to identify information-sharing processes that enhance cross-sector collaboration and communication, that improve threat pre-emption and response, and that increase the

probability of neutralizing crises before they occur. The private sector's role in information collection is voluntary and includes providing subject matter expertise and operational, vulnerability, and consequence data. Private sector partners also report suspicious activity that could signal pre-operational terrorist activity through the DHS/National Infrastructure Coordinating Center (NICC) to the DHS/National Operations Center (NOC).

FBI InfraGard: InfraGard is a partnership between the FBI, other government entities, and the private sector. The InfraGard National Membership Alliance is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants that enables the sharing of knowledge, expertise, information, and intelligence related to the protection of U.S. CIKR from physical and cyber threats.

Information shared by the private sector, including information which is protected by Protected Critical Infrastructure Information (PCII) or other approaches, is integrated with government-collected information to produce comprehensive threat assessments and threat warning products. DHS assessments, excluding PCII information, are shared across the sectors and States through electronic dissemination, posting to HSIN portals, and direct outreach by DHS staff. The private sector also reports suspicious activity through State tip lines, fusion centers, and joint terrorism task forces.

ISACs provide an example of an effective private sector information-sharing and analysis mechanism. Originally recommended by Presidential Decision Directive 63 (PDD-63) in 1998, ISACs are sector-specific entities that advance physical and cyber CIKR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external partners. ISACs typically serve as the tactical and operational arms for sector information-sharing efforts. ISAC functions include, but are not limited to, supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness. The sector partnership model recognizes that not all CIKR sectors have established ISACs. ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve.

3.2 Fusion Centers

Fusion centers are encouraged to develop or integrate operational capabilities that focus on securing CIKR and advancing Federal, State, local, and private sector CIKR protection efforts. The operational capability should include the development of analytical products, such as risk and trend analysis, and the dissemination of those products to appropriate CIKR partners. Fusion centers should be able to provide a comprehensive understanding of the threat, local CIKR vulnerabilities, the potential consequences of attacks, and the effects of risk-mitigation actions on not only the risk, but also on ongoing CIKR operations within the footprint or jurisdiction of the fusion center. CIKR protection capabilities in a fusion center will assist State, regional, and local CIKR partners in the mitigation and response to terrorist threats as well as man-made or natural hazards.

When fully equipped with CIKR protection capabilities, fusion centers should be able to assist with both information sharing and broad-based data collection. As CIKR partners, each State, region, or locality is encouraged to work with their State and local fusion centers to ensure that they understand the information-sharing requirements, so that they can develop a coordinated plan for collecting and producing the necessary information. The collection process for CIKR information should draw on various mechanisms and sources, such as existing State fusion center records or databases, open-source searches, site-assistance visits, technical systems, Federal and State resources, subject matter experts, utilization of associations (including Sector Coordinating Councils), and information shared by owners and operators.

Information exchange between Fusion Centers and CIKR partners:

- Site-specific risk information
- Interdependency information
- Suspicious activity reports
- Communications capability information
- Adversary tactics, techniques, and procedures
- Best practices
- Standard operating procedures for incident response
- Emergency contact/alert information

Please refer to the *Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers,*

Protection Capabilities for Fusion Centers), for more information and guidance on the recommended actions necessary to successfully integrate CIKR protection activities into fusion center efforts, as well as the resources available to effectively do so. The *CIKR Protection Capabilities for Fusion Centers* has been developed jointly by the DHS Office of Infrastructure Protection and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) in coordination with the National Fusion Center Coordination Group and the Criminal Intelligence Coordinating Council (provided as Appendix C to this document).

3.3 Information Protection

Effective information sharing related to CIKR relies on the balance between making information available to the appropriate authorities at all levels of government and the ability to protect sensitive or proprietary information, the disclosure of which might compromise ongoing law enforcement, intelligence, or military operations or methods. Dissemination of that information is therefore based on an end-user's homeland security responsibilities and "need to know" the information in question. Whether the sharing is "top-down" (by partners working with national-level information such as system-wide aggregate data or the results of emergent threat analysis by the Intelligence Community) or "bottom-up" (by field personnel or facility operators sharing detailed and location-specific information), the network approach places shared responsibility on all CIKR partners to adhere to applicable information-sharing protocols and practices.

The protection of sensitive infrastructure information from unauthorized disclosure is one of the most significant private sector concerns. The NIPP provides an overview of the available protection programs, but each State, local, tribal, and territorial CIKR protection plan or program should specifically address the safeguarding protocols that it will apply to the transfer, maintenance, and dissemination of collected information. It should also provide details regarding who will have access to the data, and conditions required for access. Individual States may have laws enacted to shield sensitive homeland security information from disclosure. Such laws are likely to contain specific requirements for information handling and sharing.

Protected Critical Infrastructure Information
One resource available to State, local, tribal, and territorial entities is the Protected Critical Infrastructure Information (PCII) Program. Pursuant to the Critical Infrastructure Information (CII) Act of 2002, DHS established the PCII Program in 2004 and issued a regulation (6 Code of Federal Regulations (CFR) Part 29 (the Final Rule)) setting out PCII handling and safeguarding requirements.

The PCII Program provides CIKR owners and operators with the assurance that once the information they share with the federal government is validated as PCII, it will receive all the protections of the CII Act, including exemption from public disclosure, and that it will be disseminated and safeguarded in a manner consistent with the Final Rule.

For the purposes of securing CIKR and protected systems, PCII may be shared with accredited government entities, as well as authorized Federal, State, or local government employees or contractors. Secure methods are used for disseminating PCII, which may only be accessed by authorized PCII users who have taken the PCII Program training, have a need-to-know and homeland security duties.

Types of information that may qualify for validation as PCII include, but are not limited to:

- Personal identifying information
- Vulnerability assessment reports
- Business proprietary information
- Asset identifying information
- Risk rankings
- Details of protective programs
- Threats (general and credible)

Features of the PCII Program

The PCII Program enhances private sector and government collaboration by:

- Protecting qualifying critical infrastructure information shared with the government from public release through public disclosure laws, use in civil litigation and for regulatory purposes.
- Providing a set of standard safeguarding and handling requirements for authorized users.

Benefits of the PCII Program

- The private sector can more freely share sensitive and proprietary CII with government partners with the confidence that it will be protected from public release.
- Government entities partnering with the PCII Program are better able to demonstrate their ability to safeguard private sector information from public disclosure.

PCII is currently used by numerous DHS information collection and assessment tools, including C/ACAMS, Buffer Zone Plans (BZPs), Site Assistance Visits (SAVs), and Comprehensive Reviews (CRs). The PCII Program also partners with many Federal agencies, notably the Department of Health and Human Services (HHS) and the Department of Defense (DoD). Accreditation of additional Federal, State, local, territorial, and tribal entities is ongoing.

For more information, contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

Chemical-Terrorism Vulnerability Information

On April 9, 2007, DHS issued the Chemical Facility Anti-Terrorism Standards (CFATS). Congress authorized these interim final regulations (IFR) under Section 550 of the Department of Homeland Security Appropriations Act of 2007, directing the Department to identify, assess, and ensure effective security at high risk chemical facilities. In Section 550, Congress also acknowledged DHS's need to both protect and share chemical facility security information. Consequently, DHS included provisions in the IFR to create and explain Chemical-terrorism Vulnerability Information (CVI), a new category of protected information to protect extremely sensitive information that facilities develop for purposes of complying with the CFATS that could be exploited by terrorists. At the same time, the CVI program supports sharing relevant information with State and local government officials who have a "need to know" CVI to carry out chemical facility security activities. Before being authorized to access CVI, individuals will have to complete training to ensure that the individuals understand and comply with the various safeguarding and handling requirements for CVI. More information on CFATS and CVI, including the CVI Procedures Manual, can be found at: www.dhs.gov/chemicalsecurity.

Processes for protection during information receipt, use, and storage:

- What protections, such as Protected Critical Infrastructure Information, can be applied to the information?
- Are MOUs in place that detail agreed upon information protection processes and procedures?
- If a database is used, what physical and cybersecurity measures are in place to prevent unauthorized access and release of information?
- If a file storage system is used, what physical security measures are in place to prevent unauthorized access?
- What information management processes are in place to ensure that protections are effective and appropriate?

4. Using the Risk Management Framework to Develop a Plan

The risk management framework set out in the NIPP and tailored in each of the SSPs also serves as a constructive model to build State, regional, and community CIKR protection plans and resiliency strategies. Following the framework helps ensure that all the plans are compatible and that CIKR partners can communicate clearly about the different plans. This chapter describes the intent and suggested content (high level) of each section of a State, regional, or community CIKR protection plan. Future appendices to this document will give examples of different parts of existing plans.

4.1 Introduction and Background

This section of the plan sets the baseline and helps those using the plan to understand:

- The types of infrastructure present—Which sectors are represented in the area? Are they already engaged in protective programs through DHS' Tier 1/2 program? Through sector programs?
- The relationships within and among the different sectors—Are they well-defined and organized in some way? Do they routinely work together?
- The connectivity to the SSAs and other sector CIKR partners—Does the State, region, or locality work directly with the SSAs? With the PSAs? Are they represented on the GCC, SLTTGCC, or SCC for one or more sectors?
- Has the State or local jurisdiction established their own SCCs and GCCs and, if so, how do these interact with the national level SCCs and GCCs?
- The way in which the different parties at the State, regional, or local level interact—is there a strong Homeland Security function or do you rely on the collaboration and coordination of many different agencies?
- The existing regulatory environment—do certain sectors have specific regulatory requirements at the State or local level? Does the region cross state lines and have different State requirements to address?

Developing such characterizations sets out the framework and constraints that will govern the rest of the plan. The process of gathering this information will also start building (or reinforcing) the relationships of the agencies and groups that will help to implement the plan. Further, by capturing such information in the plan, the State, region, or locality will have a reference for future use and not be as dependent on the knowledge and relationships of specific individuals.

The definitions of the individual sectors and their classes of assets, systems, networks, and functions can be found in each of the SSPs. These are the definitions that should be used in the plan—while all may not be present, the intent is to characterize the ones that are, not to redefine any of the sectors. However, the matching of the sectors to specific State or local agencies that have the responsibility for various parts of those sectors will often vary by State and locality.

The Sector Partnership Model enables unprecedented and effective coordination between government and the private sector. The plan should contain a description of sector relationships with those CIKR partners that are engaged in a State or area, such as:

- Sector-Specific Agencies
- Private sector and other owners and operators

- Department of Homeland Security
- Other Federal departments and agencies
- State and local government
- Tribal government
- Advisory councils
- Academia, research centers, and think tanks
- International organizations and foreign countries

Not all of these will apply to a particular State or region, but many will.

4.2 Setting Goals, Objectives, and Criteria

The purpose of this part of the plan is to describe the goals and objectives for a State or jurisdiction as well as the desired long-term risk management posture. The plan should also explain whether a State or jurisdiction will be applying the national criteria for significance or developing criteria specifically for the State, region, or area that would include a greater number of CIKR in the protective programs and resiliency strategies. Such criteria would recognize the infrastructure present in the area and allow for a focus on the specific sectors and CIKR that matter most. If those criteria are already developed, they can be described in the plan, so long as they do not restrict the ability to share the plan. If they are sensitive, provide a more generalized summary of the criteria, rather than the details.

The goals will describe the "steady-state" of security and risk management toward which CIKR partners will work. Goals that are collaboratively derived help CIKR partners to maintain a common vision of their desired long-term security posture. CIKR partners can use this steady-state view to best determine which specific risk-reduction and protective strategies most significantly enhance security in the area.

Well-conceived and collectively determined risk management goals will facilitate the implementation of risk-based security enhancements and resiliency strategies and will help tie regulatory requirements and voluntary efforts alike to a common end-state. They will also provide the necessary common ground to undertake a robust CIKR partnership in the future by ensuring that all CIKR partners have a common vision for the long term security posture of the State, region, or community.

The selected goals may draw from those of individual sectors, the State Homeland Security Strategy if there is one, other existing sources, or may be developed as a part of the plan. No matter which approach is taken, there should be an awareness of the other goals that already exist.

In general, goals should be limited in number and should illustrate:

- The specific risk management priorities and unique operational realities of the State, region, or community;
- Consensus on shared priorities between government and owners and operators;
- A basis for making risk management decisions and investments; and
- The necessary specificity to usefully guide decisions and yield measurable outcomes.

The plan should also include a ***Vision Statement,*** describing your overarching risk management focus and strategy. Vision statements already exist for each of the sectors—these serve as a good basis for your vision statement.

Specific goals might generally address such topics as information sharing and collaboration among CIKR partners (such as State agencies, government and the private sector, and State agencies and DHS and the SSAs), all-hazards focus, security training and awareness, reduction in key vulnerabilities, protection of critical assets, protection of cyber infrastructure, critical system resiliency and redundancy, and mitigation of cascading effects across interdependent sectors.

4.3 Identifying Assets, Systems, and Networks

This chapter of the plan explains the processes the State, region, or locality will use to identify assets, systems, and networks—and their critical functionality—and to collect information pertinent to risk management. The focus is on those assets, systems, and networks that, if damaged, would result in significant consequences—where the degree of impact on economic security, public health and safety, public confidence, loss of life, or some combination of these adverse outcomes has been established through the criteria identified in the previous section. The use of the criteria ensure that CIKR protection efforts go as deep as needed, but do not overburden limited resources by analyzing those CIKR that pose lower risks.

The critical starting point for risk analysis and management is the identification of assets, systems, and networks. This identification provides the foundation upon which to conduct risk analysis and to identify the appropriate mix of protective programs and actions that will most effectively reduce the risk to the Nation's, State's, and locality's infrastructure. "Infrastructure" includes individual assets or facilities as well as multi-asset systems and networks within and across sectors.

Sectors have assigned varying degrees of relevance and importance to account for these different levels of infrastructure. Some sectors are best represented through identification of sector systems and networks, whereas this may only be a minor consideration for other sectors. The best approach(es) for a given State or locality will likely be a combination of the approaches for the sectors that are most dominant in the area.

This section of the plan should describe the efforts for infrastructure information collection practices and methodologies that support existing governmental functions. The methodologies should ensure that the collected data are accurate, conform to taxonomy standards that enable a common understanding of the data, and meet standards for data exchange, quality and interoperability. Data standards are important for facilitating the use of data in a variety of Homeland Security applications including risk management, grants, assessment of impacts from hazards, and visualization using multiple data layers. The collected data are used to establish the Nation's critical assets as Tier 1/2 lists, for prioritizing security efforts by State, local and Federal governments. Through its participation in the Homeland Infrastructure Foundation-Level Data (HIFLD) working group, IP works with Federal, State, and local governments, and the private sector to promote domestic geospatial data collection and sharing. One critical aspect of IPs participation with HIFLD is the support in developing and disseminating the HSIP (Homeland Security Infrastructure Program) data set. The HSIP data set is comprised of geospatial infrastructure data provided by Federal and State agencies. The HSIP data are integrated in several IP applications such as C/ACAMS, iCAV and the NOC COP.

This section should also be used to describe any additional infrastructure identification and information collection efforts that might be necessary to support CIKR protection efforts—which may include using data gathered by individual sectors at a national or local level or combining the different approaches that already exist in the area.

States often have access to sector-specific information maintained by State regulatory agencies that may be appropriate for use in a national CIKR inventory. States also may have developed CIKR inventories in conjunction with other responsibilities, such as incident management and response, economic development, and the oversight of commerce and communications. Because of their CIKR-related responsibilities and authorities, States provide information that is essential in helping to identify and obtain data about assets, systems, and networks that relate to cross-sector matters.

Some of the existing approaches to consider are:

- The efforts by DHS and the SSAs to populate the Infrastructure Data Warehouse (IDW), which uses a virtual, federated database architecture to provide access to a more robust and complete infrastructure data set. The IDW will provide a larger, virtual information technology (IT) architecture to link existing, noncontiguous databases, allowing infrastructure data to remain at the source. The IDW will also provide a uniform user interface that will allow users to store and retrieve infrastructure data with a single query. This architecture will reduce duplication of effort and improve robustness of existing information at a lower cost, while facilitating data maintenance and verification by numerous partners and entities within the homeland security community.

- The work that may have been done within the State or region to implement C/ACAMS—a Web-enabled information services portal that helps State and local governments build CIKR protection programs in their local jurisdictions. Specifically, C/ACAMS provides a set of tools and resources that help law enforcement, public safety, and emergency response personnel to:
  - Collect and use CIKR asset data,
  - Assess CIKR asset vulnerabilities,
  - Develop all-hazards incident response and recovery plans, and
  - Build public/private partnerships.

  The Constellation portion of C/ACAMS is an information-gathering and analysis tool that allows users to search a range of free and subscription reporting sources to find relevant information tailored to their jurisdiction's needs. ACAMS is a secure, online database and database management platform that allows for the collection and management of CIKR asset data; the cataloguing, screening and sorting of these data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans useful to strategic and operational planners and tactical commanders. Email ACAMS-info@hq.dhs.gov if you have questions or need additional information.

- The Food and Agriculture Sector developed an assessment tool to document the most critical sector systems and subsystems. This tool is the Food and Agriculture Sector Criticality Assessment Tool (FASCAT). FASCAT helps State agencies and HSAs

identify sector elements and systems that are critical to key commodity chains or food distribution systems in their State. In addition, FASCAT allows States to:

- Prioritize vulnerability assessments and development of protective measures or mitigation strategies;
- Document and improve the characterization of their Food and Agriculture Sector risk profile; and
- Respond effectively to future DHS data calls for information on critical food and agriculture infrastructure components.

Because food and agriculture issues are often the responsibility of multiple State agencies, it is recommended that States form multi-agency working groups to identify the sector commodity systems most vital to the State. The complete FASCAT module, instructions, and an online tutorial are available at www.ncfpd.umn.edu.

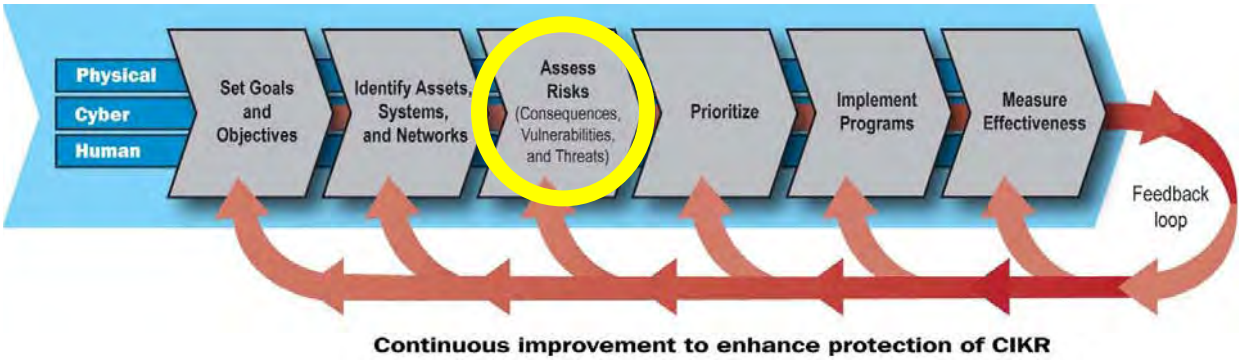
Some sectors include certain classes of assets, systems, or networks that are unlikely to be the target of an attack and/or are relatively inconsequential if attacked. These assets will not need to be identified individually unless the State or locality's criteria are much more inclusive than the national criteria.

Data sharing and protection are key challenges for DHS and the SSAs, the States, and the private sector. All CIKR partners need to work together to develop processes for collecting, storing, and verifying data that meet their individual needs and address their particular concerns—without resulting in redundant data collections by different Federal and State agencies. IICD is a key component that DHS, the SSAs, the States, and the private sector can leverage to assist with and enable data sharing. States should also determine if there are any regulatory obligations that require owners and operators to provide infrastructure data to any Federal, State, or local governmental entity. If so, this section should contain a discussion of the extent of the governmental entity's ability to share that information with the other CIKR partners identified in the plan.

Lastly, this section should include a discussion of any tools or mechanisms used by States or local entities to enable or enhance infrastructure identification and infrastructure information sharing through data visualization. Visualization provides a means to understand infrastructure asset, system, and network data in a geospatial context and allows data consumers to see how infrastructure assets relate to each other physically and from an infrastructure interdependency standpoint. Visualization tools also provide a powerful means of sharing infrastructure information within or across jurisdictional boundaries. DHS provides a free geospatial visualization tool, the Integrated Common Analytical Viewer (iCAV), to the State and local community that can be accessed via the Internet using Homeland Security Information Network (HSIN) credentials. iCAV allows State and local users to view a wide range of existing infrastructure data to inform infrastructure information collection activities, as well as an array of both static and dynamic feeds of live situational awareness information to support infrastructure analysis. iCAV also provides a limited capability to State and local users to ingest their own infrastructure data, along with DHS data and live feeds, to generate a comprehensive user- or jurisdiction-specific picture of infrastructure assets, networks, and systems. To learn how iCAV can support your organization's homeland security efforts, contact icav.info@dhs.gov. Information is also available at www.dhs.gov/iCAV.

4.4 Assessing Risks

The cornerstone of the NIPP's CIKR protection strategy is the Risk Management Framework.



This framework requires the assessment of risk to help focus CIKR protection efforts on those areas where they are needed most. Risk assessments help guide three distinct levels of protective efforts:

(1) cross-sector protection efforts, typically coordinated by DHS or State/local governments when multiple sectors of concern exist in their locations;

(2) sector- or subsector-specific protection efforts, typically coordinated by the SSA, other Federal agencies, or industry associations; and

(3) asset-, system-, or network-specific protection efforts, typically coordinated by the asset, system, or network owner or operator.

The plan should describe the processes and methodologies used to assess risk, primarily in support of the first level above, namely State, regional, or local cross-sector protection efforts. Focusing on this level will help eliminate the potential for redundancy with the risk assessment tools that are being built by DHS, the SSAs, and some of the industry associations. There may also be tools developed at the State level for one or more sectors, but these are less common except where there are regulatory requirements for such tools.

This chapter of the plan should describe the approach(es) for assessing risk[1]. It should also describe how this information will be provided to and/or shared with DHS and the SSAs as appropriate. It is expected that most of the methodologies will be ones developed by the sectors or DHS, or combinations of these, which helps ensure that these methodologies address the criteria for assessment methodologies outlined in Appendix 3A of the NIPP.

Individual sectors may have existing methodologies that are used by owners and operators; they may work with DHS and others to develop new methodologies or may use variations of methodologies, including those developed as a part of regulatory initiatives. Several methodologies or tools are likely to be used within each sector, including more detailed approaches for the assets, systems, and networks of greatest interest and simpler approaches that can be more readily used by individual owners and operators. It is possible and

[1] As defined in the NIPP, risk is a measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss. For more information on risk assessment and its role in CIKR protection, please refer to Section 3.3 of the NIPP.

appropriate to combine several risk assessment methodologies that individually comply with the NIPP risk assessment essential features (formerly the baseline criteria) to obtain the desired risk information.

It may be helpful to start with a brief discussion of any methodologies you are already using, along with those of the sectors with significant assets, systems, or networks located in your area. This should offer a high-level look at the approach being taken for risk assessment, in particular, how to draw from all the assessments that are already being done and how to fill major gaps—whether by sector or cross-sector.

Screening Infrastructure

Performing a risk assessment on an asset, system, or network can require a significant expenditure of resources by owners/operators which may not be justified in all cases. Many risk assessment methodologies suggest that some type of screening (typically a consequence screen) be performed to determine whether a full assessment is required. This helps minimize the resources devoted to full risk assessments.

A full risk assessment may be justified for all or most assets, systems, or networks in certain areas where the potential consequences associated with disruption, destruction, or exploitation are especially high. In these limited cases, a screening process is not necessary as all of the assets would "screen in." A screening process is recommended for all other infrastructure to help lower the demands on those assets, systems, and networks that may not warrant a full assessment.

The plan should describe whether a screening process would be beneficial to the State or locality and, if so, should provide details on the screening methodologies or tools currently in use or under development. Given the geographic differences across many States and communities, it is possible that screening tools might be used in more rural areas and not in major metropolitan areas.

Assessing Consequences

A consequence assessment is typically performed once an asset, system, or network has been screened and has been deemed a candidate for further review. This part of the plan should describe the consequence methodology or methodologies in use. Many sectors already have robust consequence assessment methodologies in use that can be adopted by the State or region.

This section of the plan should also address CIKR dependencies and interdependencies, and the consequences of destruction, incapacitation, or exploitation, particularly with regard to cyber elements.

Assessing Vulnerabilities

A vulnerability assessment is used to identify potential weaknesses in an asset, system, or network that could be exploited through a particular type of threat and would, in turn, result in consequences of the specified level of national, State, or regional significance or loss of critical functionality. Vulnerability assessments are described in Section 3.3.3 of the NIPP. States, regions, and localities may already be very familiar with some of the vulnerability assessments carried out by DHS in its reviews of Tier 1/2 assets and systems.

Tier1/Tier 2 Program
This program fulfills a requirement to implement recommendations of the 9/11 Commission Act of 2007. The Tier 1/Tier 2 Program maintains and annually updates a list of nationally and regionally significant assets, systems, and networks that, if disrupted or destroyed, could cause catastrophic consequences. IP, in close collaboration with CIKR partners, establishes sector-specific criteria used to identify Tier 2 assets and systems. Tier 2 assets are regionally and nationally significant CIKR; Tier 1 assets and systems are a subset of Tier 2 and are capable of causing the greatest adverse consequences. This identified subset of the Nation's CIKR focuses increased risk analysis and management attention and assures risk management activities are applied at the highest priority sites. States contribute to the identification of Tier 1 and Tier 2 assets through an annual data call.

Assessing Threats

Threat analysis determines the likelihood that an asset, system, or network will be attacked. The threat analysis section of the plan should include two elements:

General Threat Environment Description: DHS' Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) can coordinate with you during the development of the plan to develop a suitable version of this product for a public document. These descriptions are tailored to each State or locality.

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
HITRAC conducts integrated threat and risk analyses for CIKR sectors. HITRAC is a joint fusion center that spans both the Office of Intelligence and Analysis (I&A)—a member of the Intelligence Community—and IP. As called for in section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a sufficient understanding of the risks to the Nation's CIKR from foreign and domestic threats. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information in threat and risk analysis products. HITRAC also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into HITRAC's analysis.

HITRAC develops analytical products by combining threat assessments based on all source information and intelligence analysis with vulnerability and consequence assessments. The combination of intelligence and practical CIKR knowledge allows DHS to provide products that contain strategically relevant and actionable information. HITRAC coordinates closely with partners outside the Federal Government through the SCCs, GCCs, ISACs, and State and Local Fusion Centers to ensure that its products are accessible and relevant to partner needs.

As part of its Infrastructure Risk Analysis Partnership Program (IRAPP) initiative, in 2008, HITRAC launched the NY State IRAPP in coordination with the NY State Office of Homeland Security in order to assist the state with building the capability to develop a State Risk Profile.

Process for Threat/Risk Analysis: The plan should discuss the integration of the State or locality's infrastructure protection subject matter expertise with the ongoing threat analysis process—for example, threat/risk analyses that may be conducted by State Fusion Centers, as well as information from DHS and the sectors themselves.

4.5 Prioritizing Infrastructure

Critical infrastructure and protective measures should be prioritized based on risk to ensure that resources are applied where they contribute most to the mitigation of risk. Systematic methods of prioritizing assets, systems, and networks – as well as protective actions – offer

transparency and increase the defensibility of resource allocation decisions, whether they involve Federal or State funds.

This section should describe the process for risk-based prioritization of assets, systems, and networks (and the functions they all provide) within the State or community. It is important to ensure that both physical and cyber assets can be compared (i.e., through a normalization process or use of the same methodology) when prioritizing infrastructure. As with the earlier sections of this chapter, the emphasis is on prioritization within the State, region, or locality and across sectors to drive the regional, State, and local-level protection efforts.

Given that there may be many different agencies and groups with varying responsibilities in the geographic area of concern, it is important to identify:

- Party or parties responsible for performing the prioritization (e.g., HSA, specific agency leads, a combination of entities);
- Criteria for prioritization (e.g., risk, consequence, threat, surrounding population);
- Basis for prioritization (i.e., objective, quantitative information such as numerical risk assessment results, numerical consequence assessment results, etc., or subjective, qualitative information such as subject matter expert opinion);
- Frequency of prioritization efforts and updates;
- Specificity of the prioritization (i.e., Does it result in a ranked list of assets/systems/networks? Does it use bins or tiers to segregate items into high/medium/low?, etc.);
- If current prioritization process is not risk-based, the strategy/process the State or locality intends to use to migrate to a risk-based prioritization approach.

Prioritization is most effective when it considers the input from many CIKR partners. Increasing voluntary participation in both the prioritization process and the submission of risk information to support the prioritization efforts requires communicating with relevant owners and operators, building trusting relationships, and demonstrating the value of participation and collaboration. Implementation efforts at the sector level need to address all three factors to be successful.

4.6 Developing and Implementing Protective Programs and Resiliency Strategies

At the jurisdictional or regional level, CIKR protection programs serve an important coordination role as the hub of information dissemination and interaction with asset owners and operators. Consequently, CIKR protection programs should leverage external programs, such as other State and Federal CIKR protection initiatives, activities, and reports to support CIKR protection in their communities.

The plan should describe how various CIKR partners develop and implement protective programs and resiliency strategies throughout the State, region, or locality. Focus on the process used to identify, assess, select, and implement protective programs, as opposed to presenting an extensive discussion of programs and strategies currently in place; these will change with time and can be covered in appendices. An appendix may be added to the document to include detailed descriptions of the major programs that are currently underway.

To align with efforts at the Federal level, CIKR protection plans and programs should be aware of relevant activities and integration points in their communities. Representatives of Federal programs operating within the locality or region should be invited to participate in the various

coordination and collaboration meetings and asked to provide informational updates on their initiatives. For instance, DHS collaborates with SSAs and CIKR partners on a number of protective programs, initiatives, activities and reports that support CIKR protection. These activities span a wide range of efforts and include, but are not limited to:

- Buffer Zone Protection Program (BZPP)
- Site Assistance Visits (SAVs)
- Comprehensive Reviews (CRs)
- Training Programs
- Control Systems Security

DHS protective security advisors (PSAs) serve as liaisons to CIKR owners and operators, as well as State, local, and tribal officials. PSAs assist efforts to identify, assess, monitor, and minimize risk to CIKR at the regional, State, or local level. PSAs facilitate, coordinate, and/or perform vulnerability assessments in support of local CIKR owners and operators, and assist with security efforts coordinated through State homeland security advisors, as requested by State, local, or tribal authorities. 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, as well as State and local representatives. As the liaison between the field and DHS, PSAs coordinate requests for DHS assistance including training and vulnerability assessments (VAs), SAVs, BZPs, CRs; Characteristics and Common Vulnerabilities, Potential Indicators for Terrorist Attack, and Protective Measures Reports; Risk Mitigation Courses: Surveillance Detection and Soft Target Awareness, Improvised Explosive Device (IED) Awareness and Counter Terrorism Awareness; CIKR verification; and technical assistance visits.

No one party is solely responsible for development and implementation of protective programs—DHS, the SSAs, State and regional groups, local and tribal governments, and the owners and operators all have roles in implementing protective programs. Grants are often an integral part of protective programs, and Appendix A discusses how existing grant programs tie into the implementation of the NIPP and the SSPs.

As each State, region, or locality identifies and implements protective programs and resiliency strategies, it is important to recognize that one can manage risk by deterring threats, mitigating vulnerabilities, and/or minimizing consequences—and the best approach will vary by sector. Each of the SSPs sets out the approaches that are most suitable to the assets, systems, and/or networks within that sector. Each State, region, or locality may want to focus on the approaches that are the most cross-cutting, offering benefits to a number of similar infrastructure or infrastructure that are in the same geographic area.

Determining Protective Program Needs

Protective programs should match a prioritized need in order to be considered for implementation. The plan should describe the process used to identify and validate specific protective program needs. The following topics should be discussed:

- Process to identify need
- Tools used to catalogue needs
- Process to validate need and ascertain its specific characteristics
- Basis for including or excluding specific needs from protective programs
- Possible sources of funding

Describing protective programs and resiliency strategies

- Role of programs and strategies in the area's overall risk management approach
- Portion of the protective spectrum on which the sectors of interest typically focus (e.g., prevent, protect, respond, recover) and why
- Degree to which other parts of the protective spectrum are also covered
- Importance of resiliency in identifying and developing protective programs
- Identification and description of key protective programs already in place in the area, including their features, effectiveness, and sufficiency
- Process used to evaluate existing protective programs or local initiatives
- Process for assisting in the development of non-Federal protective programs
- Protective action coordination within and across sectors, as well as with DHS, other Federal departments and agencies, and State and local governments, as appropriate
- Roles and responsibilities of various security partners (e.g., DHS, SSA, owners/operators, other federal entities, State/local entities, trade associations, academia)
- Obstacles that inhibit coordination of protective programs and ways to address these challenges

Protective Program/Resiliency Strategy Implementation

This section should address implementation and maintenance of protective programs once they are prioritized. Discussion of program implementation should address the following:

- Party or parties responsible for implementation and maintenance of protective programs and resiliency strategies
- Process for coordinating specific actions with actions already taken by DHS and other CIKR partners
- Process to coordinate with the SSAs, with other States, and with DHS to implement protective actions and resiliency strategies across sectors that are required to mitigate dependencies

Performance Measurement

Key issues for the State, region, or locality will likely include:

- Determining which protective programs/resiliency strategies are considered effective and, therefore, should be supported; and
- Evaluating the effectiveness of a protective program/resiliency strategy in meeting its stated objectives.

This section should address how performance is monitored by the State or local government or regional organization, along with other CIKR partners, to determine whether they are effective, whether they have closed the gap they were intended to address, and whether they can be improved. It should describe the following:

- Process to determine which programs are successful and merit continued support
- Process to evaluate a program's effectiveness in relation to its goals
- Process to monitor technological developments that might improve or modify programs
- Processes to ensure that future decision-making will utilize information gained from program performance monitoring

Chemical Facility Anti-Terrorism Standards (CFATS)

The participation of State and local officials is integral to the success of CFATS:

- Regulated facilities are expected to coordinate with State and local officials in the development of their Site Security Plans;
- DHS will work closely with State and local law enforcement and other first responders to obtain their participation in drills and exercises at the highest risk chemical facilities;
- State Homeland Security Advisors can request lists of the high-risk chemical facilities located in their jurisdiction;
- State and local law enforcement and other first responders may receive protected facility security information upon demonstration of a need to know and certification in DHS' CVI program;
- Regionally based DHS chemical facility security inspectors will establish relationships with State and local officials that can be leveraged to help ensure the security of high risk chemical facilities during periods of increased threat, natural disasters, and other extenuating circumstances;
- Support the development of the national risk picture by assisting in identification, assessment, monitoring, and minimizing risk to critical chemical assets at the local or state level;
- Facilitate, coordinate, and/or perform technical assistance visits for local critical infrastructures and key resources;
- Provide guidance on established security practices;
- Convey local concerns and sensitivities of CFATS covered facilities to DHS and other Federal agencies;
- Work with DHS to verify, validate and investigate CFATS related incident; and
- Provide local context and expertise to DHS on CFATS covered facilities.

4.7 Measuring Progress

Measuring progress is a critical part of the NIPP risk management framework; it not only documents progress but also supports continuous improvement and fine tuning of various risk assessment and protective program efforts. Measurement of progress is the shared responsibility of all CIKR partners, including DHS, individual SSAs, States, localities, and individual owners and operators. While DHS focuses on measuring progress across all CIKR sectors, each SSA is responsible for measuring progress for its own sector or sub-sectors. Similarly, each State or locality needs to address progress in its specific area.

The plan should address how the State, region, or locality and its CIKR partners will collect and verify the data needed to report on progress. The plan should also describe how this information is used to support continuous improvement in CIKR protection and risk mitigation efforts. This effort should be closely tied to the other metrics efforts underway in the sectors. The State, region, or locality may contribute primarily to the sector and national metrics that are already being collected or they can also be developing similar but additional measures to capture information on progress in protecting CIKR that have State, regional, or local significance, even if they do not have national significance. Measurements may also be defined by the State Homeland Security Strategy and/or various grant programs that are providing funds.

If State, regional, or local metrics are being defined, the process being used should be decribed. Some governments and organizations may have the ability to collect and verify information pertinent to CIKR protection by using processes that serve the purposes of pre-

existing programs. Legal or regulatory limitations may prohibit the use of this information for anything other than its original purpose. In these cases, this section should detail both the pre-existing process, as well as the information collection process that will be used to collect information that may be reported to DHS and others.

HSPD-7 requires SSAs to provide the Secretary of Homeland Security with annual reports that serve as a primary tool for assessing performance and reporting on progress. Not only would these sector reports be more robust if they contained information from various States, regions, and communities, but new reporting requirements are being defined each year. The need for an annual report from each State is foreseeable.

Implementation Actions

Each State, locality, or regional group should identify and track the specific actions associated with both the formation and execution of their CIKR protection function and the specific, prioritized programs that they are implementing. Preparing and using a list of implementation actions will help to facilitate consistent and thorough tracking and identification of specific actions.

The implementation actions should encompass all relevant activities undertaken by the different CIKR partners. The lists of actions will also facilitate conversations with other States and communities, with the SSAs, with DHS, and with owners and operators. Major actions that are performed by CIKR owners and operators are just as important as Federal, State, and local government activities. Major actions performed by these owners and operators may include projects sponsored by multiple private sector CIKR partners or those actions coordinated by a trade association, academia, or a research consortium. Duplicative data collection efforts may be a pitfall of multiple partner information collection. This will necessitate increased communications with the SSAs and DHS.

One purpose of measuring progress is to allow CIKR partners at all levels to make decisions that are informed by the results of past efforts and by the status of ongoing efforts. The implementation of the measures and metrics detailed in this section will provide CIKR partners with valuable tools for making future decisions and for tracking progress toward the goals established. This section should describe how metrics will be used to guide future decisions. Specifically, it should address:

- Procedures for incorporating metrics into the decision-making process;
- How metrics will be used to measure progress toward goals;
- The process for determining whether or not metrics indicate CIKR protection activities are on track;
- The process for addressing insufficient progress toward identified goals; and
- Challenges in developing and using metrics and plans to address these challenges (e.g., challenges presented by voluntary participation in protective program implementation).

Addressing these issues will ensure that appropriate feedback is provided to all stages of the risk management framework, supporting continuous improvement of risk management efforts.

5. Cybersecurity Considerations

Cyber infrastructure[2] enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CIKR sectors. This network enables services such as the Internet and financial markets, and also controls many critical processes, including the electric power grid and chemical processing plants. A spectrum of malicious actors can and do conduct attacks against cyber infrastructure on a continuous basis. Of primary concern is the risk of organized cyber attacks capable of causing debilitating disruption to the Nation's critical infrastructure, economy, or national security. Although a debilitating attack against the Internet has not been launched yet, the increasing ease with which powerful cyber attack tools can be obtained and used places the ability to conduct cyber attacks within reach of most groups or individuals wishing to do harm to the United States.

The 18 CIKR Sectors' functions and services are enabled through the cyber infrastructure; however, if cybersecurity is not integrated appropriately, the risk to sectors' missions is greatly increased. DHS and other public and private sector CIKR partners collaborate to enhance cybersecurity awareness and preparedness efforts and increase the resilience of the Nation's cyber infrastructure. Responsibility for cybersecurity is shared across public and private sector entities, including State and local governments, and individual citizens. DHS' National Cybersecurity Division (NCSD), the Nation's focal point for cybersecurity, is committed to working with SLTT government entities to enhance the Nation's cybersecurity posture and offers a variety of cybersecurity resources and technical assistance to help SLTT governments address cybersecurity as part of national and State CIKR protection efforts. As SLTT government entities establish and enhance their own CIKR protection function they should consider the following strategies and approaches related to cybersecurity.

- **Raise awareness of cyber risk and the importance of implementing cybersecurity practices.** A critical element of national efforts to enhance cybersecurity is making the public aware of cyber threats and the role that the Federal Government, State and local governments, the private sector, and individual citizens play in protecting the cyber infrastructure. SLTT government entities should work to ensure that their employees receive annual cybersecurity awareness training commensurate with employees' responsibilities. DHS and other organizations offer training related to cybersecurity and control systems security that can be used to provide a foundation for SLTT government training. SLTT governments should also sponsor cybersecurity awareness programs that target individual citizens, small businesses, and other constituents. Finally, cybersecurity experts across SLTT government entities should work to raise awareness of elected and appointed officials in all branches of SLTT governments on the role of cybersecurity in CIKR protection.
- **Develop and implement cybersecurity policies, plans, and procedures.** State governments should develop and implement cybersecurity policies, plans, and procedures that set the vision, goals, and objectives for State-wide cybersecurity. These policies, plans, and procedures should be made available to local jurisdictions and local jurisdictions should be encouraged to adapt them for their own use. Effective

[2] *National Infrastructure Protection Plan*, Page 13, The Cyber Dimension: Cyber infrastructure includes electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure. Information and communications systems are composed of hardware and software that process, store, and communicate. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

policies, plans, and procedures will enable SLTT governments to build effective partnerships, share policy and operational information, assess and manage risk, and respond to and recover from cyber-related events.

- **Build and maintain relationships with CIKR partners.** SLTT government entities are a vital component of the Nation's cyber preparedness capability and contribute to the information sharing, capacity building, and coordination efforts necessary for preparing for, responding to, and recovering from a cyber event. SLTT government entities should establish and maintain relationships with Federal departments and agencies, other SLTT government entities, the private sector, academia, and international organizations with cybersecurity expertise. Building and maintaining strong cooperative relationships with Federal government departments and agencies, CIKR Information Sharing and Analysis Centers (ISAC), the Multi-State ISAC (MS-ISAC), [3] and numerous associations that focus on State homeland security concerns, enable SLTT governments to gain access to cybersecurity resources and expertise and enhance the flow of information. Groups such as the National Governor's Association, National Emergency Management Association, and National Association of State Chief Information Officers (NASCIO) are valuable resources for SLTT governments and provide avenues for broadening participation in CIKR protection efforts. Local governments should explore the establishment of relationships with one another to leverage each other's cybersecurity resources and capabilities.
- **Share and obtain information through established policy and operational mechanisms.** SLTT government entities should ensure that they are receiving threat and vulnerability information pertaining to not only physical and human threats but cyber threats. Establishing and maintaining relationships with the United States Computer Emergency Readiness Team (US-CERT)[4] at DHS, the MS-ISAC, other ISACs and information-sharing organizations can ensure access to valuable cyber threat and vulnerability information. In addition, SLTT organizations should report cyber incidents to US-CERT to obtain technical assistance. Ensuring that information and intelligence is shared among Federal and SLTT government organizations is an essential component of protecting the Nation's CIKR. The establishment of State and Local Fusion Centers (SLFCs) across the Nation also provides a mechanism for the two-way flow of timely, accurate, actionable, all-hazard information between State and local governments and intelligence and law enforcement communities.[5] SLTT organizations are encouraged to leverage SLFCs to obtain and share information related to cyber threats.
- **Identify cyber assets, systems, networks, and functions.** SLTT government entities should consider what role cyber infrastructure plays in supporting key SLTT

[3] Multi-State Information Sharing and Analysis Center (MS-ISAC) http://www.msisac.org/

[4] The U.S. Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the Nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities; disseminating cyber threat warning information; and coordinating incident response activities. US-CERT engages with Federal departments and agencies, industry, the research community, State and local governments, and others to disseminate reasoned and actionable cybersecurity information to the public. State and local government personnel can sign up for cyber alerts, tips, and other public information on how to better protect cyber networks and access tools and training by visiting www.us-cert.gov.

[5] SLFCs are multidisciplinary information-sharing hubs that bring together Federal, State, and local governments, law enforcement, and the private sector. During a regional or national event, SLFCs are intended to be central mechanisms for coordinating intelligence, resources, and situational awareness across the various levels of governments and with the private sector.

government functions by identifying cyber assets, systems, networks, and functions that exist within SLTT government entities and jurisdictions. Efforts to identify cyber assets, systems, networks, and functions should consider whether the SLTT government is operationally dependent on the cyber infrastructure or if the cyber infrastructure is enabling a support function (e.g., exchanging mission data versus non-operational e-mail) and determine whether the cyber infrastructure is owned/operated/provided by the SLTT government or the private sector. DHS' Tier 1/ 2 Program provides an avenue for SLTT governments to identify cyber assets, systems, networks, and functions. State HSAs should coordinate with State Chief Information Officers and State Chief Information Security Officers to ensure that appropriate IT/cyber assets, systems, networks, and functions are identified and included in Tier 1/ 2 submissions.

- **Implement a risk management program.** SLTT governments rely on cyber infrastructure to fulfill their missions and should assess the risk[6] to critical functions supporting key government operations and services. The assessment should serve as a key component of an entity's overall risk management program that enables informed decision making and efficient allocation of resources. DHS' IP conducts vulnerability assessments that provide an avenue for SLTT governments to identify physical, human, and cyber vulnerabilities affecting CIKR in their jurisdictions. Risk assessment efforts should leverage recognized cybersecurity methodologies, standards, and best practices.[7] SLTT governments should leverage established relationships and partnerships to obtain and share threat and vulnerability information to inform risk assessment and risk management efforts at all levels (i.e., local, regional, and national). State and local government officials are also encouraged to collaborate with key State stakeholders (e.g., Chief Information Officers and Chief Information Security Officers) and information-sharing fora such as the MS-ISAC, other CIKR ISACS, and NASCIO to exchange perspectives on best practices for assessing vulnerability.
- **Develop and enhance cybersecurity operational capabilities.** States without a cybersecurity incident response team (CSIRT) should develop this capability and leverage the lessons learned and best practices of other States. Where possible, local governments should also ensure that they have a relationship with a State CSIRT. SLTT governments, specifically State Chief Information Officers and Chief Information Security Officers and their State Cyber Security Incident Response Teams should consider participating in the Government Forum of Incident Response and Security Teams.[8]
- **Exercise and test cybersecurity policies, plans, and procedures and operational capabilities.** Exercises (e.g., full-scale, functional, tabletop, etc.) should be used to test

---

[6] Risk is a function of threats to, vulnerabilities of, and consequences of the compromise or exploitation of the infrastructure.
[7] DHS' National Cybersecurity Division collaborated with public and private sector security partners to develop the *Cyber Security Vulnerability Assessment (CSVA).* This tool allows organizations to self-assess their overall cybersecurity posture by evaluating an organization's cybersecurity policies, plans, and procedures. It consists of approximately 100 multiple choice questions across ten categories. Based on the responses, the CSVA identifies effective practices and suggests options that an organization or facility can implement to enhance their cybersecurity posture. The CSVA leverages concepts from recognized standards, guidance, and methodologies from organizations such as the International Organization for Standardization, the Information Systems Audit and Control Association, and the National Institute of Standards and Technology.
[8] The Government Forum of Incident Response and Security Teams (GFIRST), sponsored by NCSD/US-CERT, contributes to protecting national CIKR by increasing the level of information sharing among government IT and cybersecurity incident response professionals responsible for protecting cyber infrastructure. By creating a trusted and open environment through a horizontal network of government cyber incident first responders with deep knowledge of cyber threats to CIKR and means to mitigate those threats, GFIRST increases the situational awareness across the Nation and helps to ensure cyber incident response capabilities are driven by actionable data and informed decisions.

policies, plans, and procedures to ensure an appropriate level of preparedness and response to cyber events. Exercises that produce lessons learned and corrective action plans can improve incident response and operational capabilities when corrective actions are implemented. SLTT government entities should work with NCSD's Cyber Exercise Program to explore a cyber exercise for their State that is tailored to meet State needs and structures. The Cyber Exercise Program employs scenario-based exercises that focus on risks to the cyber and information technology infrastructures. State officials should also consider participating in the DHS-sponsored bi-annual national cyber exercise known as Cyber Storm, a multi-day exercise that allows Federal agencies, States, private sector, and international partners to exercise their cybersecurity response capabilities and builds awareness about the importance of cybersecurity in CIKR protection.

DHS, specifically NCSD, is available to work with State and local governments as they develop new or enhance existing CIKR protection plans to ensure they address cybersecurity issues and fully leverage available Federal and CIKR sector resources.

6. Coordinating CIKR Protection R&D Efforts

HSPD-7 establishes an annual requirement for a national R&D plan for CIKR protection. DHS' Directorate for Science and Technology (S&T) develops this plan in partnership with the White House Office of Science and Technology Policy (OSTP) on the same schedule as the National CIKR Protection Annual Report. The National Critical Infrastructure Protection (NCIP) R&D Plan is the result of a collaborative process undertaken by the Federal CIKR protection community as well as CIKR partners from the sectors. This process involves collecting information on R&D requirements from a broad range of CIKR partners, and then prioritizing those requirements based on risk.

DHS S&T established Integrated Product Teams (IPTs) to coordinate the planning and execution of R&D programs together with the eventual hand-off to maintainers and users of project results. IPTs constitute the transition portfolio of DHS S&T, targeting deployable capabilities in the near term. IPTs generally include the research and technology perspective, the customer and end user perspective, and an acquisition perspective. The customer and end users monitor and guide the capability being developed; the research and technology representatives inform the discussions with scientific and engineering advances and emerging technologies; and the acquisition staff help transition the results into practice by the maintainers and end-users of the capability.

The IPT topic areas reflect the capability requirements of homeland security stakeholders. The current IPTs operated by DHS S&T are listed below. Each sponsors projects that are relevant to the infrastructure protection mission. The three bolded IPTs are co-chaired by the DHS IP office.

Information Sharing/Management	**Counter IED**
Border Security	Cargo Security
Chem/Bio Defense	People Screening
Maritime Security	**Infrastructure Protection**
Cybersecurity	Preparedness & Response: Incident Management
Transportation Security	Preparedness & Response: Interoperability

States and localities can contribute to the requirements and prioritization process by working with the SLTTGCC as well as the relevant individual sectors. They should also work with DHS, the SSAs, local universities and research organizations, as well as private companies to identify research that may be underway in their jurisdictions (or elsewhere) to fill gaps in protective programs. Certain States may also have their own research programs, particularly in sectors like Agriculture and Food or Water.

States should be aware of what programs are underway, and should engage with key efforts to ensure that their particular needs and concerns are included in each project's specifications. Individual State agencies may have the greatest affinity for specific R&D efforts.

7. Managing CIKR Protection Programs and Activities

Best Practices in Building a CIKR Protection Program from Operation Archangel*

- Define a strategic vision that includes attainable goals and objectives and aligns the community's needs and concerns with overarching National Priorities.
- Establish leadership that is driven, proactive, persuasive, and results-oriented.
- Obtain support from "champions" within the community, such as multidisciplinary agency and local government leaders.
- Establish a forum for engaging public and private sector partners, including asset owners, operators, security managers, and other multi-discipline CIKR partners as a mechanism for obtaining early buy-in.
- Convene a team of dedicated personnel to participate in the program.
- Demonstrate regional collaboration and resource sharing.

*Operation Archangel was developed by the Los Angeles Police Department to identify and protect critical infrastructure and key resources in the Los Angeles metropolitan area. Its purpose is to defend likely targets against catastrophic terrorist attacks. Archangel is based on the guiding principle that local member agencies are most knowledgeable about their own critical assets.

7.1 Program Management Approach

Each State, region, or locality is likely to manage its homeland security responsibilities differently. CIKR protection activities may be centralized in one agency (e.g., Homeland Security, Public Safety, or Emergency Management) or spread across different agencies (including the Departments of Public Health, Environmental Protection, and Agriculture as well as the Public Utilities Commission), or entirely ad hoc. Therefore, it is important that the management processes the State or locality has established and/or will establish to support its responsibilities under the NIPP are defined and specific as to how the State or locality will ensure those responsibilities are satisfied. The roles and responsibilities of different parties should be defined, along with coordination mechanisms. This is potentially even more complex when multiple States and/or combinations of private sector and government CIKR partners are involved in regional frameworks.

The State, region, or locality should determine how it intends to staff and manage its NIPP-related responsibilities over the short and long term. There are several approaches including:

- Creation of a program management office that is devoted specifically to the development and implementation of the plan and program. This approach works well when focus is needed and when resources permit.
- Embedding of the CIKR protection management function and responsibilities into an existing program management office. This approach works well when another office is already set up and when funding allocations can be determined.
- Assignment of different processes and responsibilities to various State or local agencies. This approach is suitable when funding is limited (or embedded in other programs) and the visibility of a separate office is not needed.

Regardless of the alternative that is selected, the State, region, or locality will need to describe the philosophy and the structure of its approach to managing CIKR protection. They should also describe how key processes will be implemented and monitored. The most suitable approach may change over time; thus, it will be important to periodically assess the effectiveness and suitability of its chosen organizational approach.

7.2 Plan Maintenance and Update

The State, region, or locality should define when and how its CIKR protection plan will be updated. For example, it might be updated:

- When there is a critical change in the definition of assets, systems, networks, or the functions they provide to reflect the implications of those changes
- On an annual basis to reflect significant changes during the period since the last update
- On a triennial basis for a complete review in conjunction with the update of the NIPP or the SSPs
- Continuously as milestones change
- As part of completing the annual reporting requirements
- Whenever there is a new initiative
- When methodologies and tools are developed

All updates should be made through a collaborative process involving the sector CIKR partners. There should be a defined version control process along with editing rights, to provide consistency in voice, tone, and content, and ensure that the right updates and changes to the plan are provided to those who need such information.

7.3 Annual Reporting

The National CIKR Protection Annual Report now includes annual reports from both the SLTTGCC and the Regional Consortium Coordinating Council (RCCC.) These reports are prepared with input from various CIKR partners and serve as a primary tool for assessing performance and reporting on progress. The annual reports:

- Provide a common vehicle across States, regions, localities, tribal communities, and territories to communicate CIKR protection performance and progress to CIKR partners and other government entities;
- Establish a baseline of existing CIKR protection programs and initiatives;
- Identify priorities;
- Determine and explain how CIKR protection efforts at various levels support the national effort;
- Provide an overall progress report for the SLTTGCC and RCCC and measure that progress against the national CIKR protection goals;
- Provide feedback to DHS, the CIKR sectors, and other government entities that will be used as the basis for continuous improvement of the CIKR protection program; and
- Help to identify and share best practices from successful programs.

Starting in 2009, the draft annual reports are due on May 1 of each year, with final reports due June 1. It is expected that individual inputs to the SLTTGCC and RCCC annual reports will be due roughly one to two months prior to the May 1st submission deadline to allow time for compiling the annual report.

7.4 Education, Training, and Outreach

The successful implementation of the NIPP and the SSPs, as well as State, regional, or local CIKR protection plans, relies on building and maintaining individual and organizational CIKR

protection expertise. Training and education in a variety of areas are necessary to achieve and sustain this level of expertise. An effective training program will result in:

- An increase in the amount of voluntary participation by owners and operators, and
- A more comprehensive exchange of information on private sector CIKR programs.

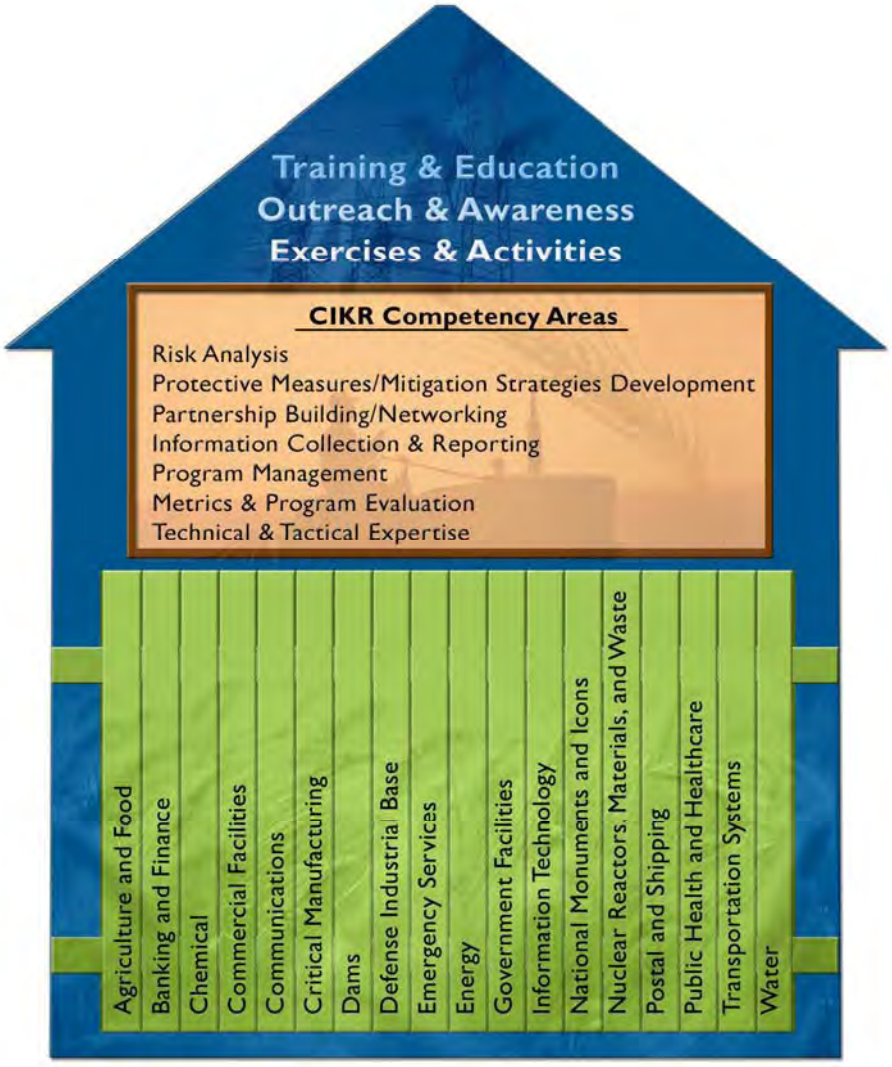
The plan should include processes to address:

- The types of training that would be useful for certain members of the State, region, or locality to receive (e.g., risk management, physical security, cost-benefit analysis, cybersecurity). This should take into consideration any specialized knowledge necessary for effective CIKR protection in the area.
- The types of awareness initiatives that are underway or are planned to inform different audiences on human, physical, and cyber issues for CIKR protection.
- The categories of individuals within the area that would benefit from training or education (e.g., asset owner/operators; Chief Security Officers; facility security personnel; State personnel; third party auditors) and the rough number of individuals or entities needing the training.
- The types of CIKR protection training, education, certification, or other programs currently available. You should also seek to identify any gaps that should be filled and describe the strategy for filling those gaps.

Before the State, region, or locality develops training and education programs of its own, it is important to understand what materials, courses, and programs are already available from DHS, the SSAs and their sectors, trade associations, universities, and others. To assist in understanding the available resources, DHS is developing an inventory of training programs and recently conducted a training and education needs assessment. Together, the needs assessment and the inventory will result in a prioritized set of training requirements for DHS to address. The courses, webinars, online materials, and videos that are produced may help to address some of your specific training requirements. These materials will range from awareness-level videos and online courses to more comprehensive courses on a number of infrastructure protection topics (such as risk methodologies) to webinars on focused topics of interest. The figure below depicts some of the competencies that are beneficial when developing and implementing CIKR protection plans and programs.

It is important to share education and training requirements with DHS as well as the SSAs and their sectors because what benefits one State, region, or locality is likely to be useful to many others as well. In such cases, it is likely that DHS or the SSAs will help address the State, region, or locality's specific training requirements—but may not be able to meet your exact timelines.

Additionally, a list of training courses that have been approved by FEMA for use of eligible DHS grant funds is located at https://www.firstrespondertraining.gov/odp%5Fwebforms/.



7.5 Implementation Plans

In general, effective implementation of the plan and program will require specific, task-oriented implementation plans that have broad buy-in with sufficient fidelity to allow CIKR partners to accomplish critical activities on a clear, appropriate, and well-defined time scale. Implementation plans can also be effective mechanisms for capturing and communicating additional details on implementation activities and overcoming issues.

The table below provides an outline for a detailed implementation plan and can also serve as a checklist for those States, regions, and localities not using formal implementation plans. Not all implementation plans will need this level of detail, particularly for efforts that are largely completed or conducted primarily by private sector CIKR partners.

Suggested Elements of an Implementation Plan	
Scope	▪ Goal/objective and context ▪ Governance arrangements setting out accountability mechanisms ▪ Summary of the major activities that will be undertaken to achieve the goal/objective and associated assumptions, constraints, and exclusions ▪ Criteria against which implementation and progress toward objectives can be monitored and assessed ▪ Benefits statement identifying the intended beneficiaries and expected benefits to be evaluated
Work breakdown	▪ Work breakdown structure or process flow, covering phases and related activities, start and end dates, and responsibilities ▪ Implementation schedule by fiscal year
Resources	▪ Resource table showing estimated roll-out of deliverables and costs by fiscal year
CIKR partner engagement	▪ List of key CIKR partners for each major phase/activity ▪ Roles and responsibilities for key CIKR partners ▪ Strategy and timeline for consultation with key CIKR partners
Contracting and procurement	▪ Procurement plan summarizing the items and/or services (i.e., outputs) for which external providers will be sought, including anticipated cost and internal accountability ▪ Strategy for securing and managing important agreements
Quality assurance	▪ Monitoring and evaluation strategy ▪ Quality assurance strategy

Key implementation activities and timelines related to NIPP implementation should include:

- Review NIPP and establish processes needed to support NIPP implementation
  90 days after revised NIPP is approved (expected in 2009)
- Review and revise CIKR-related plans as needed to reinforce linkage between NIPP steady-state CIKR protection and NRF incident management requirements
  180 days after revised NIPP is approved
- Review current CIKR protection measure to ensure alignment with HSAS threat conditions and specific threat vectors/scenarios
  180 days after revised NIPP is approved
- Review and, as appropriate, revise training programs to ensure consistency with NIPP requirements
  180 days after revised NIPP is approved

These implementation timelines are from Appendix 2B of the original (2006) NIPP and serve as mechanisms for all CIKR plans to ensure that they remain current with each version of the NIPP and national CIKR protection efforts. Should a jurisdiction just be developing their initial plan now, they should coordinate based on the 2006 NIPP until the 2009 version is released.

Appendix A – Coordinating with Grant Programs

Efforts to support the protection of CIKR are an essential component of any overarching homeland security program. In accordance with the NIPP risk management framework, as well as the benchmarks and requirements identified in the Homeland Security Grant Program (HSGP), State governments should build and sustain a statewide/regional CIKR protection program. This program should 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 *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, local, tribal, territorial, and sector-specific homeland security strategies. Achieving that national priority requires meeting objectives that include understanding and sharing information about terrorist threats and other hazards, building CIKR partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. To achieve these efforts, CIKR partners should have the following in place:

- Coordinated, risk-based CIKR plans and programs 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 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; and
- Access to robust information-sharing networks that include relevant intelligence, threat analysis, and real-time incident reporting.

In support of the previously described efforts, one of the core missions of DHS is to enhance the ability of State, local, and tribal governments to prevent, protect against, respond to, and recover from terrorist attacks and other disasters. FEMA's comprehensive suite of grant programs is an important part of the Department's larger, coordinated effort to strengthen homeland security preparedness. These programs implement objectives addressed in a series of post-9/11 laws, strategy documents, plans, and HSPDs. Five preparedness programs within FEMA's comprehensive grants portfolio are:

- Homeland Security Grant Program (HSGP)
  - State Homeland Security Program (SHSP)
  - Urban Areas Security Initiative (UASI)
  - Metropolitan Medical Response System (MMRS)
  - Citizen Corps Program (CCP)
- Tribal State Homeland Security Program (SHSP Tribal)
- Nonprofit Security Grant Program (NSGP)
- Operation Stonegarden Grant Program (OPSG)
- Regional Catastrophic Planning Grant Program (RCPGP)

Additional grant programs that may be leveraged to support related homeland security and emergency preparedness activities include:

- Buffer Zone Protection Program (BZPP)
- Emergency Management Performance Grant (EMPG)
- Emergency Operations Center (EOC) Grant Program
- Interoperable Emergency Communications Grant Program (IECGP)
- Intercity Bus Security Grant Program (IBSGP)
- Port Security Grant Program (PSGP)
- Regional Catastrophic Preparedness Grant Program (RCPGP)
- Transit Security Grant Program (TSGP)
- Trucking Security Program (TSP)

Together, these grants programs[9] may fund a wide range of homeland security and emergency preparedness activities, to include planning, organization, equipment purchase, training, exercises, and management and administration costs. These programs support objectives outlined in the National Preparedness Guidelines and related national preparedness doctrine, such as the NIMS, NRF, and the NIPP. A detailed description of each of these programs can be found at http://www.fema.gov/grants.

[9] This reflects the Fiscal Year (FY) 2008 preparedness grant program portfolio and is subject to change in future years.

Appendix B – DHS Programs and Resources

The following programs offer tools and resources for States, regions, and localities to apply on their own or in conjunction with DHS. Many of these are also described in the main body of this guide.

B.1 Vulnerability Assessment Program

The Vulnerability Assessment (VA) Program supports IP's mission to reduce the risk to the Nation's CIKR by conducting, validating, and tracking vulnerability assessments of the Nation's most critical assets and systems. The success of the Program requires integrating and leveraging capabilities and resources between the government and the private sector. Only through this integration can a comprehensive national protective architecture be fully established.

The objectives and expected outcomes of the VA Program include the identification, prioritization, and protection of the Nation's CIKR. These objectives and outcomes will be achieved through assessing vulnerabilities, providing recommended protective measures, and by coordinating and partnering with SSAs, other Federal agencies, and State, regional, local, tribal, territorial, and private sector CIKR partners. The VA Program will provide CIKR partners with the tools, processes, and methodologies to streamline security investment decisions and reduce vulnerabilities. The Program will also facilitate information sharing and CIKR awareness through developing, maintaining, and expanding Characteristics and Common Vulnerabilities (CV), Potential Indicators of Terrorist Activity (PI), and Protective Measures (PM) reports for dissemination to CIKR partners. Additionally, the VA Program will provide vulnerability and consequence analysis of CIKR in support of special events and exercises.

The VA Program serves as DHS' focal point for strategic planning, coordination, and information sharing in the planning and execution of vulnerability assessments of the Nation's CIKR. Through the development and deployment of a scalable assessment methodology, and tracking the development of protective measures of other Federal, State, local, tribal, territorial, and private sector CIKR partners, the VA Program supports the implementation of the NIPP and HSPD-7 by identifying vulnerabilities, supporting collaborative security planning, and recommending protective measures and risk mitigation strategies.

The following paragraphs contain brief descriptions of some of the programs and tools used to conduct vulnerability assessments. The list represents core programs, and should not be considered as an all-inclusive list.

Comprehensive Review (CR)

The CR is a cooperative, government-led analysis of CIKR facilities or systems. The CR incorporates potential terrorist attack scenarios, the consequences of an attack, and the integrated preparedness and response capabilities of the owner or operator and emergency service organizations. The results are used to enhance the overall security posture of the facilities or systems, the surrounding communities, and the geographic region using short-term enhancements and long-term risk-based investments in training, processes, procedures, equipment, and resources for State and local stakeholders. The CR process relies on Federal, State, local, tribal and territorial partnerships to achieve nationally coordinated, and State and locally executed, capabilities for infrastructure protection and incident response.

Site Assistance Visit (SAV)

The SAV is a vulnerability assessment conducted jointly by DHS in coordination and cooperation with Federal, State, local, tribal, territorial, and private sector facilities stakeholders. The SAV uses a hybrid methodology of dynamic and static vulnerabilities including elements of asset-based approaches (identifying and discussing critical site assets and current security postures) and scenario-based approaches (assault planning and likely attack scenarios to ensure current threats are included). Through SAVs, DHS informs CIKR owners and operators of protective measures that would increase the ability to detect and prevent terrorist attacks, and provides options for reducing vulnerabilities. A SAV can range from a "quick visit" to a full security vulnerability assessment—three to five days to comprehensively assess physical, cyber, and system interdependencies. SAVs assemble consequence and vulnerability information to support the collection of data for risk analyses. Results are provided to the owner or operator through a SAV Report. Since FY04, over 900 SAVs have been conducted.

Characteristics and Common Vulnerabilities (CV), Potential Indicators of Terrorist Activity (PI), and Protective Measures (PM) Reports

CV, PI, PM reports identify common vulnerabilities of critical infrastructure and the types of terrorist activities that likely would be successful in exploiting these vulnerabilities. The VA Program has developed Integrated Infrastructure Papers to integrate over 300 individual reports, which are currently available to over 1000 Federal, State, local and private sector partners on a secure website.

Buffer Zone Protection Program (BZPP)

The BZPP is a DHS administered grant program designed to support local law enforcement (LLE) and owners and operators of CIKR increase security in the "buffer zone" – the area outside of a facility that can be used by an adversary to conduct surveillance or launch an attack. The BZPP brings LLE, facility owners and operators, Federal, State, local, territorial, and tribal stakeholders together to develop a Buffer Zone Plan (BZP). The BZP identifies specific threats and vulnerabilities associated with a facility and its assets. LLE needs the tools to prepare, prevent, defend, and mitigate the impacts of a terrorist attack, and through this grant program, grants go directly to LLE to obtain the approved BZP equipment, training, and other resources they need.

B.2 Bombing Prevention

The Office for Bombing Prevention (OBP) is dedicated to enhancing and coordinating the Nation's ability to detect, deter, prevent, and respond to attacks that use improvised explosive devices (IED) against CIKR and soft targets. To achieve this goal, OBP is actively engaged in three primary areas: coordinating national and intergovernmental bombing prevention efforts; conducting requirements, capabilities, and gap analyses; and promoting information sharing and bombing prevention awareness. OBP serves as DHS' lead agent for ensuring that diverse nationwide prevention programs function together efficiently to meet evolving bombing threats. Additionally, OBP works to empower law enforcement, first responders, the private sector, and the public through information sharing and awareness of IED threats. OBP current activities include coordinating the DHS IED Working Group, supporting Homeland Security Presidential Directive 19 implementation, implementing Multi-Jurisdiction IED Security Planning, and conducting capabilities analysis using the National Capabilities Analysis Database. OBP provides important information sharing through TRIPwire.

TRIPwire, the Technical Resource for Incident Prevention (www.tripwire-dhs.net), is DHS' online, collaborative, information-sharing network for bomb squad, law enforcement, and other emergency services personnel to learn about current terrorist IED tactics, techniques, and procedures, including design and emplacement considerations. Developed and maintained by OBP, the system combines expert analyses and reports with relevant documents, images, and videos gathered directly from terrorist sources to assist law enforcement anticipate, identify, and prevent IED incidents.

OBP will deliver the TRIPwire Community Gateway (TWCG) and the TRIPwire Field Tool. The TWCG is a new TRIPwire web portal designed specifically for the Nation's CIKR owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent IED incidents. Developed and maintained by OBP, TWCG shares IED related information tailored to each of the 18 sectors of CIKR, in accordance with the NIPP. Sector partners benefit from increased communication, improved awareness of emerging threats, and access to resources and guidance on specific IED preventive and protective measures for their facilities and requirements. The TRIPwire Field Tool is a portable productivity platform to deliver TRIPwire and other bombing prevention and response resources to TRIPwire users in the field. Operators will now have the latest IED-related information readily available in a secure, encrypted information-sharing environment.

B.3 Protective Security Advisor Program

To better partner with State governments, local communities, and businesses, DHS placed a national presence, Protective Security Advisors (PSAs), in local communities throughout the country to assist with local efforts to protect critical assets. As individuals averaging 20 years of law enforcement, military, and anti-terrorism experience, PSAs are recruited from, live, and work in local communities. PSAs provide a Federal resource to communities and businesses to assist in the protection of our Nation's CIKR and further State and local homeland security initiatives.

In 2004, DHS established the PSA program, deploying a cadre of 68 critical infrastructure security specialists to 60 metropolitan areas designated as PSA districts across the United States. In order to represent DHS at the Federal, State, local, tribal, and territorial levels, PSAs were deployed to provide DHS with a local perspective to the national risk picture. PSAs support the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical assets at the regional and local levels. PSAs serve as DHS' on-site CIKR and vulnerability assessment specialists, and as a vital channel of communication between officials and private sector owners and operators.

Through their strategic deployment across the United States, PSAs are often the first DHS personnel to respond to incidents involving CIKR. Consequently, PSAs are uniquely able to provide early situational awareness to DHS and IP leadership during an incident, often performing duties as the Infrastructure Liaison at the Joint Field Office in support of the Principal Federal Official. As the vital facilitators of communications between local responders and DHS, PSAs also coordinate requests from CIKR owners and operators for services and resources to include training, scheduling of SAVs, BZPs, CRs, and verification and technical assistance visits.

PSAs interact and coordinate with a large number of individuals and organizations at all levels of government and the private sector. PSAs regularly interact with State Homeland Security

Advisors (HSAs), Emergency Management Directors, and other private sector, Federal, State, local, tribal, and territorial entities, as well as other DHS components. PSAs also work with Federal Bureau of Investigation (FBI) special agents to conduct joint site visits and vulnerability assessments of high-consequence CIKR assets.

Given the initial success of the PSA program and levels of support required for 68 field personnel, IP management identified the need to develop a more robust PSA leadership structure. In order to optimize efficient management of the PSA program while achieving its overarching objectives as directed by Congress, the program has expanded its field-deployed personnel to 76 PSAs. Ten additional PSAs will be added in FY 09 which will provide at least one field-deployed PSA in each State, bringing the total number of PSAs to 86.

B.4 Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

HITRAC is a joint program office integrating the intelligence expertise of the Office of Intelligence and Analysis and the infrastructure protection mission of IP. Together, analysts from these two offices work together to produce integrated threat and risk analysis products for use by public and private sector decision makers. HITRAC coordinates closely with both the Intelligence and infrastructure protection communities, to ensure its products are relevant to partner needs, and informed by the best information available to the Federal government.

HITRAC also manages a number of programs designed to inform strategic planning in the infrastructure protection community, including:

- **Integrated Risk Analysis Program:** Conducts national, cross-sector, sector-specific, regional, State, and site-specific risk analyses and assessments to aid decision-makers with planning and prioritizing risk-reduction measures within and across the CIKR sectors. These analyses and assessments leverage a number of analytic approaches, including the Strategic Homeland Infrastructure Risk Assessment process, which is used to develop the National and Sector Risk Profiles.
- **National CIKR Prioritization Program:** HITRAC works with CIKR partners to identify and prioritize the assets, systems, and networks most critical to the Nation through the Tier 1/Tier 2 List for critical assets, systems, networks, nodes, and functions within the United States, and the Critical Foreign Dependencies Initiative (CFDI) for those same CIKR located outside of the United States. The prioritized lists of CIKR are used to guide the Nation's protective and incident management responses, such as the various homeland security grant programs.
- **Infrastructure Risk Analysis Partnership Program (IRAPP):** IRAPP assists partners interested in pursuing their own CIKR risk analysis, whether in the Federal, State, local, or private sector CIKR protection communities. IRAPP involves customized support to interested partners, and the sharing of best practices across the CIKR protection community.

HITRAC analysts also conduct classified and unclassified outreach to public and private sector partners, bringing information to decision makers to aid their understanding and ability to tackle the critical national and homeland security challenges they face.

B.5 Homeland Security Information Network (HSIN)

HSIN is a robust and significant information-sharing system that supports NIPP-related, steady-state CIKR protection and NRF-related incident management activities, as well as serving the

information-sharing processes that form the bridge between these two homeland security missions. The linkage between the nodes results in a dynamic view of the strategic risk and evolving incident landscape. HSIN functions as one of a number of mechanisms that enable DHS, SSAs, States/regions/territories/localities, and other partners to share information. By offering a user-friendly, efficient conduit for information sharing, HSIN enhances the combined effectiveness of all CIKR partners in an all-hazards environment. HSIN architecture design is informed by experience gained by DoD and other Federal agencies in developing networks to support similar missions. It supports a secure common operating picture for all security partner command or watch centers, including those of supporting emergency management and public health activities.

HSIN is composed of multiple, non-hierarchical communities of interest (COIs) that offer CIKR partners the means to share information based on secure access. COIs provide virtual areas where groups of participants with common concerns, such as law enforcement, counterterrorism, critical infrastructure, emergency management, intelligence, international, and other topics, can share information. This structure allows government and industry partners to engage in collaborative exchanges, based on specific information requirements, mission emphasis, or interest level.

B.6 Critical Infrastructure Warning Information Network (CWIN)

CWIN is a relatively new mechanism that facilitates the flow of information, mitigates obstacles to voluntary information sharing by CIKR owners and operators, and provides feedback and continuous improvement for structures and processes. CWIN is the critical, survivable network connecting DHS with vital sector partners that are essential to restoring the Nation's core infrastructure. Those sectors/subsectors are Communications, IT, and Electricity, as well as their Federal and State official counterparts. In the circumstance where all or a major part of telecommunications and Internet connectivity are lost or disrupted, CWIN is designed to provide a survivable “out of band” communications and information-sharing capability to coordinate and support infrastructure restoration. Once the core capabilities of telecommunications, the Internet, and electricity are restored, normal communication channels can be utilized and other CIKR can begin the process of restoration.

B.7 Protected Critical Infrastructure Information (PCII)

One resource available to State, local, tribal, and territorial entities is the PCII Program. The PCII Program provides CIKR owners and operators with the assurance that once the information they share with the Federal Government is validated as PCII, it will receive all the protections of the Critical Infrastructure Information (CII) Act of 2002, including exemption from public disclosure and use in regulatory proceedings. In addition, once DHS validates the information as PCII, it will be disseminated and safeguarded in a manner consistent with the implementing PCII regulation at 6 C.F.R Part 29. Secure methods are used for disseminating PCII, which may only be accessed by authorized Federal, State, local, or tribal government employees or contractors who have homeland security duties and a need to know the PCII. A PCII authorized user is an individual who has taken the PCII Program training.

The PCII Program enhances private sector and government collaboration by protecting qualifying CII shared with the government from public release through public disclosure laws, use in civil litigation and for regulatory purposes. It also provides a set of standard safeguarding and handling requirements for authorized users. This allows the private sector to more freely share sensitive and proprietary CII with government partners with the confidence that it will be

protected from public release. In addition, government entities partnering with the PCII Program are better able to demonstrate their ability to safeguard private sector information from public disclosure.

For more information, contact the PCII Program Office at pcii-info@dhs.gov. Additional PCII Program information may also be found at www.dhs.gov/pcii.

B.8 Constellation/Automated Critical Asset Management System (C/ACAMS)

C/ACAMS is a Web-based information services portal that enables State and local governments to build and implement CIKR protection programs in their local jurisdictions. Specifically, C/ACAMS provides a set of tools and resources that enables law enforcement, public safety, and emergency response personnel to:

- Collect and use CIKR asset data;
- Assess CIKR asset vulnerabilities;
- Develop all-hazards pre-incident response and recovery plans; and
- Build public/private partnerships.

The Constellation portion of C/ACAMS is an information-gathering and analysis tool that allows users to search a range of free and subscription-reporting sources to find relevant information tailored to their jurisdiction's needs. ACAMS is a secure, online database and database management platform that allows for the collection and management of CIKR asset data; the cataloguing, screening, and sorting of these data; the production of tailored infrastructure reports; and the development of a variety of pre- and post-incident response plans useful to strategic and operational planners and tactical commanders. Access to the C/ACAMS information technology (IT) system is granted following successful completion of the CI/KR Asset Protection Technical Assistance Program (CAPTAP).

B.9 CIKR Asset Protection Technical Assistance Program (CAPTAP)

CAPTAP assists State and local law enforcement, first responders, emergency managers, and homeland security officials to understand: the basic tenets of the NIPP; the value of a comprehensive State and local infrastructure protection program; and 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.

DHS provides a Train-the-Trainer (TTT) program for individuals from their respective States to become certified CAPTAP instructors; this program is highly recommended for those individuals with previous experience as an instructor. Individuals interested in becoming CAPTAP instructors must first complete the initial CAPTAP curriculum. Individuals who complete the TTT program are provided with all the necessary instructor-related media and must follow the DHS standard operating procedures on holding regular CAPTAP services in their States. To inquire about obtaining CAPTAP training for your State, please email ACAMS-info@hq.dhs.gov. C/ACAMS Program information may also be found at https://www.dhs.gov/acams.

B.10 Integrated Common Analytical Viewer (iCAV)

DHS provides iCAV to the State and local community as a free tool to enable infrastructure data visualization in a geospatial context. iCAV allows State and local users to view a wide range of existing Federal infrastructure data sets to inform infrastructure analysis and

information collection activities. iCAV also allows users to access and integrate a wide array of both static and dynamic data feeds to provide live situational awareness for decisionmaking. iCAV provides a limited capability to State and local users to ingest their own infrastructure data to generate a comprehensive, fused, user- or jurisdiction-specific picture of infrastructure assets, networks, and systems. This fusion provides DHS, States, and local jurisdictions and the private sector with a rapid, common understanding of the relationships between events and infrastructures to support coordinated event risk mitigation, preparedness, response, and recovery activities. iCAV can be accessed via the Internet using Homeland Security Information Network (HSIN) credentials. For more information contact icav.info@dhs.gov. Information is also available at www.dhs.gov/iCAV..

B.11 Chemical Facility Anti-Terrorism Standards (CFATS)

Section 550 of the DHS Appropriations Act of 2007 grants the Department the authority to regulate chemical facilities that "present high levels of security risk." The CFATS Interim Final Rule, published April 9, 2007, establishes a risk-based approach to screening and securing chemical facilities determined by DHS to be "high risk." In order to make that determination, CFATS requires facilities in possession of specific quantities of DHS-defined Chemicals of Interest (COI) to complete a Top-Screen questionnaire. After reviewing the Top-Screen, DHS determines which facilities are preliminarily high risk. The CFATS regulation then requires each preliminary high risk facility to submit a Security Vulnerability Assessment (SVA). The facilities still considered high risk after a review of their SVA are provided a final tier and required to complete a Site Security Plan (SSP) that meets DHS' risk-based performance standards. CFATS does allow some chemical facilities to submit Alternative Security Programs (ASPs) in lieu of DHS' SVA and SSP. Certain types of facilities (e.g., facilities regulated under the Maritime Transportation Security Act) are exempt under Section 550 and CFATS.

Any facility that manufactures, uses, stores or distributes any of the DHS COI at or above a specified quantity, and does not fall into an exemption, must complete and submit a Top-Screen questionnaire as a first step in complying with CFATS. Facilities that are required to comply with at least some provisions of the CFATS regulation will largely fall into the following categories:

- chemical manufacturing, storage, and distribution;
- energy and utilities;
- agriculture and food;
- paints and coatings;
- explosives;
- mining;
- electronics;
- plastics;
- universities and research institutions; and
- healthcare and pharmaceuticals.

In Section 550, Congress also acknowledged DHS's need to both protect and share chemical facility security information. Consequently, DHS included provisions in the IFR to create and explain Chemical-terrorism Vulnerability Information (CVI), a new category of protected, extremely sensitive information that facilities develop for purposes of complying with the CFATS that could be exploited by terrorists. The CVI program allows sharing of relevant

information with State and local government officials who have a "need to know" CVI to carry out chemical facility security activities. Before being authorized to access CVI, individuals will have to complete training to ensure that the individuals understand and comply with the various safeguarding and handling requirements for CVI. More information on CFATS and CVI, including the CVI Procedures Manual, can be found at: www.dhs.gov/chemicalsecurity.

B.12 Risk-Based Performance Standards

Section 550 directed the Department to issue regulations "establishing risk-based performance standards for the security of high risk chemical facilities." CFATS establishes Risk-Based Performance Standards (RBPSs) for security issues such as perimeter security, access control, personnel surety, and cyber security. However, not all high risk facilities will need to take action to satisfy each RBPS. A facility's SSP will be tailored to its specific tier level, security issues, risks, and circumstances, as determined by DHS' review of its SVA.

B.13 National Infrastructure Coordinating Center (NICC)

The NICC is a 24/7 watch/operations center that maintains ongoing operational and situational awareness of the Nation's CIKR sectors. As a CIKR-focused element of the National Operations Center (NOC), the NICC provides a centralized mechanism and process for information sharing and coordination between the government, SCCs, GCCs, and other industry partners. The NICC receives situational, operational, and incident information from the CIKR sectors, in accordance with information-sharing protocols established in the NRF. The NICC also disseminates products originated by HITRAC that contain all-hazards warning, threat, and CIKR protection information:

- *Alerts and Warnings:* The NICC disseminates threat-related and other all-hazards information products to an extensive customer base of private sector partners.
- *Suspicious Activity and Potential Threat Reporting:* The NICC receives and processes reports from the private sector on suspicious activities or potential threats to the Nation's CIKR. The NICC documents the information provided, compiles additional details surrounding the suspicious activity or potential threat, and forwards the report to DHS sector specialists, the NOC, HITRAC, and the FBI.
- *Incidents and Events:* When an incident or event occurs, the NICC coordinates with DHS sector specialists, industry partners, and other established information-sharing mechanisms to communicate pertinent information. As needed, the NICC generates reports detailing the incident, as well as the sector impacts (or potential impacts), and disseminates them to the NOC.
- *National Response Planning and Execution:* The NICC supports the NRF by facilitating information sharing among SCCs, GCCs, ISACs, and other partners during CIKR mitigation, response, and recovery activities.

B.14 National Exercise Program (NEP)

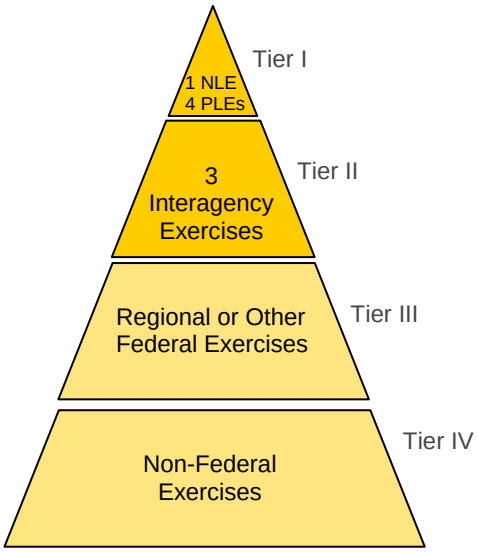
DHS provides overarching coordination for the NEP to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition to the incident management framework established in the NRF. NEP program components include:

- **National Level Exercise -** an annual national security and/or homeland security exercise centered on White House-directed, U.S. Government-wide strategy and policy

- **Principal Level Exercise (PLE) -** a quarterly cabinet level exercise focused on current U.S. Government-wide strategic issues
- Five-year schedule of NLE/PLE and significant NEP Tiered exercises with a strategic U.S. Government-wide focus
- **National Exercise Schedule (NEXS) -** a schedule of all Federal, State, and local exercises
- **Corrective Action Program (CAP) -** administered by DHS in support of the Homeland Security Council and the National Security Council, involves a system and process for identifying, assigning, and tracking remediation of issues.
- **Homeland Security Exercise and Evaluation Program (HSEEP) -** DHS policy and guidance for designing, developing, conducting, and evaluating exercises. Provides a threat and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to help States and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises.

The NEP categorizes exercise activities into four tiers. These tiers reflect the relative priority for interagency participation, with Tier I as the highest and Tier IV the lowest. US Government exercises are assigned to tiers based on a consensus interagency judgment of how closely they align to US Government-wide strategic and policy priorities.

- **Tier I Exercises (Required).** Tier I exercises are centered on White House-directed, U.S. Government-wide strategy and policy-related issues and are executed with the participation of all appropriate Cabinet-level Secretaries or their Deputies and all necessary operations centers. NLEs and Cabinet Level Exercises (CLEs) constitute Tier I and there are five NEP Tier I exercises annually. Examples include the Top Officials and Eagle Horizon (COOP) exercises.



- **Tier II Exercises (Required).** Tier II Exercises are focused on strategy and policy issues supported by all appropriate departments and agencies either through the National Simulation Cell (Center) or as determined by each department or agency's leadership. Tier II exercises are endorsed through the NEP process as meriting priority for interagency participation. Tier II exercises take precedence over Tier III exercises in the event of resource conflicts. The PTEE PCC shall recommend no more than three Tier II exercises for interagency participation annually. An example of a Tier II exercise is the Ardent Sentry, an annual terrorism exercise focused on defense support to civil authorities that is jointly sponsored by the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (NORTHCOM). Ardent Sentry has been integrated with the DHS National Homeland Security Exercise Program and is held concurrently with the TOPOFF exercises.
- **Tier III Exercises (Permitted).** Tier III Exercises are other Federal exercises focused on operational, tactical, or organization-specific objectives and not requiring broad interagency headquarters-level involvement to achieve their stated exercise or training objectives.

- **Tier IV Exercises.** Tier IV Exercises are exercises in which State, local, tribal, and/or territorial governments, and/or private sector entities, are the primary training audience or subject of evaluation.

B.15 Maritime Assessment and Strategy Toolkit (MAST) Technical Assistance Program

The program links distribution of funds to participation in a port-wide risk management planning process. This process combines the USCG's Maritime Security Risk Analysis Model (MSRAM) with the FEMA Grant Programs Directorate's own Special Needs Jurisdiction Toolkit to allow port areas to develop risk management strategies that will assist them in identifying the most cost-effective projects, an essential step in prioritizing risks and facilitating a port-wide risk management planning process. MAST serves to further enhance the existing Area Maritime Security Plans and also allow for ports to better integrate their security efforts into the broader planning construct that forms the core of the Urban Areas Security Initiative.

B.16 Transit Risk Assessment Module (TRAM) Technical Assistance Program

The purpose of the Program Risk Assessment delivery is to enable agencies to: prioritize needs in terms of security countermeasures, emergency response capability enhancements, and recovery capability enhancements based on terrorist threats and risk; develop a road map for future mass transit agency funding allocations for terrorist attack risk reduction; and prepare for future Federal funding requirements. This assistance is intended for Mass Transit officials and their allied agencies involved in Homeland Security and Emergency Management. The program provides a Technical Assistance Team to support the agency with assessments; leverages existing threat/vulnerability assessments to the extent possible; provides on-site technical experts in risk assessment and emergency response; and applies the methodology and toolkit for the agency in conjunction with the local representatives.

B.17 Maritime Transportation Security Act

This law requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures; security patrols; establishment of restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment. The Act creates a consistent security program for all the Nation's ports to better identify and deter threats and promotes better coordination on waterfront security between local port security committees and Federal agencies. MTSA required the establishment of committees in all the Nation's ports to coordinate the activities of all port stakeholders, including other Federal, State, and local agencies, industry, and the boating public. These groups, called Area Maritime Security Committees, are tasked with collaborating on plans to secure their ports so that the resources of an area can be best used to deter, prevent, and respond to terror threats.

MTSA also specifies that all U.S. port facilities deemed at risk for a "transportation security incident," such as liquefied natural gas marine terminals, fossil fuel processing and storage facilities, and cruise ship terminal facilities, must prepare and implement security plans for deterring such incidents to the "maximum extent practicable." MTSA requirements also extend to offshore oil and gas facilities (other than deepwater ports) that host more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more, or produce more than 100,000 barrels of oil per day or 200 million cubic feet per day of natural gas.

Appendix C – Critical Infrastructure and Key Resources Protection Capabilities for Fusion Centers

Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers

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

July 2008

State, Local, Tribal and Territorial
Government Coordinating Council

TABLE OF CONTENTS

Critical Infrastructure and Key Resource Protection Capabilities for Fusion Centers

I. PURPOSE

This document identifies the capabilities necessary for State and Major Urban Area Fusion Centers (Fusion Centers) to establish a Critical Infrastructure and Key Resource (CIKR) protection analytic capability that supports infrastructure security activities at the State and local level. 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). 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 1-4, 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.

II. 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

[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.

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 multi-disciplinary 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 on not only the risk, but also on business operations within the private sector.

III. FUSION CENTER CIKR 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

Structure of the *Baseline Capabilities Document*

I. *Intelligence Cycle Capabilities - The Intelligence Cycle is defined in the National Criminal Intelligence Plan and incorporated in Guideline 1 of the Global Justice Fusion Center Guidelines. For purposes of Baseline Capabilities, the titles are expanded to be:*
   A. Planning and Requirements Development;
   B. Information Gathering/Collection;
   C. Intelligence Analysis and Production;
   D. Intelligence/Information Dissemination; and
   E. Re-evaluation

II. *Management and Administrative Capabilities:*
   A. Management and Governance;
   B. Security;
   C. Information Privacy Protections;
   D. Information Technology/Communications Infrastructure, Systems, and Equipment;
   E. Facility Location, Personnel, and Physical Infrastructure; and
   F. Funding

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*.

I. Intelligence Cycle Capabilities

A. Planning and Requirements Development

The following capabilities address the plans, and their associated policies, standards, 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.)

1. **Fusion Centers shall ensure relevant CIKR information and analysis is included in the required Statewide/Regional Risk Assessment, which 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 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), Alert, Warning, and Notification, and Situational Awareness), 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/Regional Risk Assessment, and the center's defined Information Requirements. [See BC #I.A.7.][2] The system(s), such as the Constellation/Automated Critical Asset Management System (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;

[2] Refer to BC II.E.1 on guidance to further develop plans for access to data sources based on the Fusion Center's defined mission and core business process.
[3] See page 15 for background on the Constellation/Automated Critical Asset Management System (C/ACAMS)

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; and
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

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 which are used for receiving, cataloging, and retaining information provided to the center (as called for by BC# I.B.3), to ensure CIKR-related information is appropriately stored and protected.**

C. Intelligence Analysis and Production

1. **Fusion Centers shall update their production plans, as called for in section I.C.1 of the *Baseline Capabilities Document*, to incorporate CIKR-related analysis and develop products for CIKR stakeholders which enhance the protection of critical infrastructure.**

2. **Consistent with section I.C.8 of the *Baseline Capabilities Document*, Fusion Centers shall consider assigning at least one analyst to the CIKR analysis function on a full-time basis.**

[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 16 for more details.

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.C.9]**
    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; and
    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. Liaison with CIKR partners and other agencies to identify emerging threats, de-conflict 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 like 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 co-located with other analysts within the Fusion Center; and
    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 SAR's that are determined to be Information Sharing Environment-SAR (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 to provide 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 de-conflict 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]

In addition to the requirements for analyst training outlined in section I.C.4 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).

D. Intelligence/Information Dissemination

1. **Fusion Centers shall incorporate CIKR stakeholders into the dissemination plan required by section *I.D.1, Baseline Capabilities Document.***
   a. The dissemination plan shall identify the processes and protocols for ensuring CIKR information is disseminated to appropriate government authorities and CIKR owners and operators consistent with the pre-established 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 are provided to affected industry sectors.

2. **Consistent with section II.D.3., *Baseline Capabilities Document,* Fusion Centers shall ensure relevant CIKR analysis is reported to DHS Homeland**

[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.

[6] The SLTTGCC is currently working with the DHS Office of Infrastructure Protection on creating a CIKR-specific training curriculum for analysts.

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.

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:**
   a. Ensure that technology assisted dissemination used is appropriate for the level of classification;
   b. That unclassified distribution utilizes technologies that have become ubiquitous and easy to use for all recipients;
   c. That 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)

E. Re-evaluation

1. **In accordance with the Baseline Capability document (section I.E) 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?
   c. Do they believe the products to be accurate?
   d. Have the products motivated them to take concrete actions?
   e. Do the products contain appropriate contextual background?

[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.

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

g. Does the product address an anticipated event?

II. Management and Administrative Capabilities

A. Management and 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 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 Capability 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), 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 official responsible for CIP activities and the DHS Protective Security Advisor.
   c. Follow all procedures outlined for section II.A.3. of the *Baseline Capability Document* for each stakeholder, particularly the requirements for Memorandum of Understanding (MOU), and if necessary, a Non Disclosure Agreement (NDA)
   d. Information exchange between Fusion Centers and security partners shall include information pertaining to:
      i. Site-specific security risks;
      ii. Inter- and intra-sector 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; and
      viii Emergency contact / alert information.

4. **Fusion Centers shall review and update their policies and procedures manual, to ensure 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 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.E]**

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, and 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 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 on going/periodic basis; and
   g. Access timely information on recommended pre-incident prevention and preparedness best practices and activities.

F. Funding

1. **No additional capabilities required**

[8] See Page 14 for more information on the Homeland Security Information Network-Critical Sectors (HSIN-CS)

IV. 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 which 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 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, and 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: 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 4: 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 tearline reports[9] as appropriate.

Step 5: Re-evaluation

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.

The steps in this CIKR intelligence cycle are shown below:

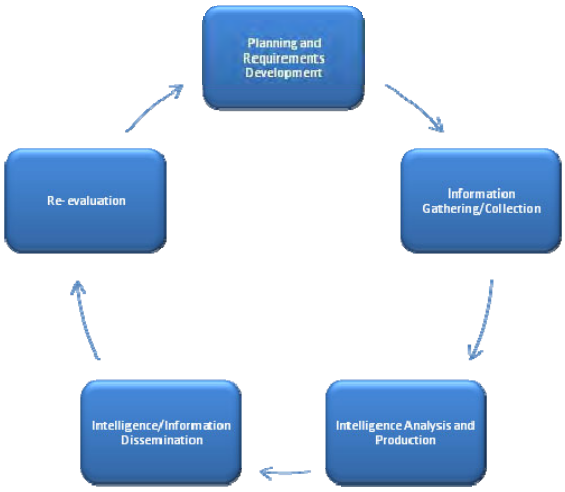


Figure 1 - The CIKR Intelligence Operations Cycle

Integrating the CIKR capability into state and local Fusion Centers will aide in the development of products which enable and support federal, state, local, and private sector decision-making.

[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.

V. 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 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 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; and
- Builds upon the NIMS, which provides a consistent template for managing incidents.

There are a number of components within DHS which help facilitate the objectives of the NIPP and the NRF at the regional, state and local level. 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 (IA)**

IA is the Executive Agent for the State and Local Fusion Center Program within the Department of Homeland Security. Their 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. They lead 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.

IA has many valuable resources that could be tapped by a Fusion Center's CIP capability. They include:

- Ability to provide Fusion Centers 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 multi-level 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; and
- 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

• **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 compliment 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 their 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 which

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 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, serving as liaisons between DHS, the private sector, and federal, state, territorial, local, and tribal entities. PSAs act as DHS' 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; and
- 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.

- **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, access PCII and only use it 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 Services 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, prevent, respond 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 Information Protection (TRIP*wire*)** – *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 anticipate, identify, and prevent IED incidents.

IP resources also offer analytic resources and products that can be used as reference 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 Department of Homeland Security's Intelligence-Infrastructure Protection Fusion Center, comprised of analysts from the both 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' 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: pre-planned long-term analyses, pre-planned 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 IA and the 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 (100+ technical assistance deliveries already made to support state and local Fusion Center efforts); and
- Various training programs (Thousands of state / local officials have already participated in DHS-sponsored or approved training).

- **FEMA Grant Programs Directorate (GPD)**

- Grant Funding (they have already provided over $250 million dollars to states and urban areas between fiscal year (FY) 2004 and FY 2007 in support of intelligence and information sharing activities)

Federal Bureau of Investigations (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 website and a secure, clientless virtual private website, 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.

VI. THE PATH FORWARD

Ultimately, protection and preparedness can only be 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 nation 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*[10] and is 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 that the center operates – some have adopted an "All Crimes" approach, others have also included an "All Hazards"[11] approach. The *National Strategy* 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, co-location 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 Department of Homeland Security, the 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.

[10] The *National Strategy for Information Sharing* was developed in partnership with Global and other State and local officials, to include Fusion Center officials.

[11] See glossary of *Baseline Capabilities Document* for definition of All Crimes Approach and All Hazards Approach.

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 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 resource protection activities should not be considered a baseline capability. Accordingly the document was edited to limit baseline capabilities to ensuring the center:

1. Can disseminate alerts, warnings, and notifications and other relevant analytic reports to the affected critical infrastructure or private sector entity; and
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 Resource 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 FY 2006 and 2007 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; and
- Access to robust information-sharing networks that include relevant intelligence, threat analysis, and real-time incident reporting12.

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 supports achievement of the Expanded Regional Collaboration and Strengthen Information Sharing and Collaboration national priorities noted in the National Preparedness Guidelines.

Therefore, it is strongly encouraged that Fusion Centers 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, but 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 preventive and protective measures to deter, disrupt, and/or mitigate threats.

[12] National Preparedness Guidelines

Homeland
Security