

Appendix 5: Integrating CI/KR Protection as Part of the Homeland Security Mission

Appendix 5A: State, Local, and Tribal Government Considerations

State, local, and tribal efforts support the implementation of the NIPP and associated SSPs by providing a jurisdictional focus and enabling cross-sector coordination. The NIPP recognizes that there is not a one-size-fits-all approach to CI/KR protection planning at the State and local levels. Creating and managing a CI/KR protection program for a given jurisdiction entails building an organizational structure and mechanisms for coordination between government and private sector entities that can be used to implement the NIPP risk management framework. This includes taking actions within the jurisdiction to set security goals; identify assets, systems, and networks; assess risks; prioritize CI/KR across sectors; implement protective programs; and measure the effectiveness of risk-mitigation efforts. These elements form the basis of CI/KR protection programs and guide the implementation of relevant CI/KR protection-related goals and objectives outlined in State, local, and tribal homeland security strategies.

This appendix provides general guidance that can be tailored to unique jurisdictional characteristics, organizational structures, and operating environments at the State, local, and tribal levels.

The NIPP is structured to avoid redundancy and ensure coordination between State, local, and Federal CI/KR protection efforts. States or localities are encouraged to focus their efforts in ways that leverage Federal resources and address the relevant CI/KR sector's protection requirements in their particular areas or jurisdictions. This appendix outlines a basic framework to guide the development of CI/KR protection strategies, plans, and programs in coordination with the NIPP.

To align with the NIPP, State and local CI/KR protection plans and programs should explicitly address six broad categories regarding their CI/KR protection approach:

- CI/KR protection roles and responsibilities;
- Building partnerships and information sharing;

- Implementing the NIPP risk management framework;
- CI/KR data use and protection;
- Leveraging ongoing emergency preparedness activities for CI/KR protection; and
- Integrating Federal CI/KR protection activities.

5A.1 CI/KR Roles and Responsibilities

The NIPP outlines a set of broad roles and responsibilities for State, regional, local, and tribal entities (see chapter 2). State, regional, local, and tribal CI/KR protection plans (or elements addressing CI/KR in State or local homeland security plans or strategies) should describe how each jurisdiction intends to implement these roles and responsibilities. In particular, jurisdictions should consider and describe in their plans the following:

- Which offices or organizations in the jurisdiction perform the roles or responsibilities outlined in the NIPP or supporting SSPs;
- Whether gaps exist between the jurisdiction’s current approach and those roles and responsibilities outlined in the NIPP or in an SSP, and how the gaps will be addressed;
- Whether any roles and responsibilities should be revised, modified, or consolidated to accommodate the unique operating attributes of the jurisdiction;
- How the jurisdiction will maintain operational awareness of the performance of the CI/KR protection roles assigned to different offices, agencies, or localities; and
- How the jurisdiction will coordinate its CI/KR protection roles and responsibilities with other jurisdictions and the Federal Government.

5A.2 Building Partnerships and Information Sharing

Effective CI/KR protection requires the development of partnerships, collaboration, and information sharing between government and private sector owners and operators. This includes maintaining awareness of CI/KR owner and operator concerns, disseminating relevant information to owners and operators, and maintaining processes for rapid response and decisionmaking in the event of a threat or incident involving CI/KR within the jurisdiction. To address partnership building, networking, and information sharing, State and local entities should determine whether the appropriate mechanisms for sharing information and networking with security partners are in place. If mechanisms are not established at all of the relevant levels, State and local entities should identify means for better coordinating and sharing information with security partners. Options to be considered and described in State, regional, local, and tribal CI/KR protection plans can include, but are not limited to:

- Ensuring collaboration with other government entities and the private sector using a process based on the partnership model outlined under the NIPP or an abbreviated form of the model addressing just those sectors that are most relevant to the jurisdiction;
- Instituting specific information-sharing networks, such as an information-sharing portal, for security partners in the jurisdiction. These types of networks allow owners and operators, and governmental entities to share best practices, provide a better understanding of sector and cross-sector needs, and inform collective decisionmaking on how best to utilize resources;
- Developing standing committees and work groups to discuss relevant CI/KR protection issues;

- Developing a regular newsletter or similar communications tool for CI/KR owners and operators on relevant CI/KR protection issues and coordination within the jurisdiction; and
- Participating in existing sector-wide and national information-sharing networks, including those offered by trade associations, ISACs, SCCs, and threat warning and alert notification systems.

The information-sharing approach for a given jurisdiction will vary based on CI/KR ownership, number and type of CI/KR sectors represented in the jurisdiction, and the extent to which existing mechanisms can be leveraged. The options presented above are merely a description of some available mechanisms that jurisdictions may consider as they develop the organization of their programs and document their processes in a CI/KR protection plan.

5A.3 Implementing the Risk Management Framework

The NIPP risk management framework described in chapter 3 provides a useful model for State, regional, local, and tribal jurisdictions to use in addressing CI/KR protection within the given jurisdiction. The process provides a risk-based approach that can help State and local entities to identify, prioritize, and protect CI/KR assets and systems within their jurisdictions. This process also allows State and local jurisdictions to enhance coordination with DHS and the SSAs in developing and implementing CI/KR protection programs. The following should be considered when developing CI/KR protection programs:

- What are the jurisdiction’s goals and objectives for CI/KR protection? How do these goals relate to those of the NIPP and the SSPs that are relevant to the jurisdiction?
- What are the CI/KR assets, systems, networks, and functions within the jurisdiction or that impact the jurisdiction? Are there significant interstate or international dependencies or interdependencies? Are any of the assets, systems, or networks within the jurisdiction deemed to be nationally critical by DHS?
- Are risk assessments for CI/KR within the State being conducted or planned by DHS, SSAs, or owners and operators in accordance with the processes outlined in the NIPP? Is there a need for the jurisdiction to conduct additional or supplemental risk assessments? Do the methodologies for conducting risk assessments address the baseline criteria outlined in chapter 3?
- What are the CI/KR protection priorities within the jurisdiction? How do these priorities correlate with the national priorities established by the Federal Government? How do these priorities correlate with the ongoing CI/KR protection priorities established for each sector at the national level?
- What actions or initiatives are being taken within the jurisdiction to address CI/KR protection? How do these relate to the national effort?
- What types of metrics will be used to measure the progress of CI/KR protection efforts?

5A.4 CI/KR Data Use and Protection

States and other jurisdictions may employ a variety of means to collect CI/KR data or respond to CI/KR data requests. State, regional, local, and tribal plans should outline how the jurisdiction has organized itself to address CI/KR data use and protection. The following issues should be considered in developing the CI/KR protection plan:

- Will the jurisdiction maintain a comprehensive database of CI/KR in the State, region, or locality? How will the jurisdiction collect such information?

- How will sensitive data that may be in the possession of State, local, or tribal governments be legally and physically protected from public disclosure, and what safeguards will be used to control and limit distribution to appropriate individuals?
- Will data collection mechanisms be compatible and interoperable with the NADB to enable data sharing?
- How will the jurisdiction ensure that it is maintaining current information?
- Will data requests from the Federal Government for CI/KR data be channeled to the owners and operators through the States?
- Are there local legal authorities and policy directives related to data collection? Are these authorities adequate? If not, how will the jurisdiction address these issues?

5A.5 Leveraging Ongoing Emergency Preparedness Activities for CI/KR Protection

The emergency management capabilities of each State and local jurisdiction are an important component of improving overall CI/KR protection. States and localities should look to existing programs and leverage ways in which CI/KR protection can be integrated into ongoing activities. Areas to be considered when drafting a CI/KR protection plan include:

- Does the jurisdiction's exercise program account for CI/KR protection? If not, how will the State or locality incorporate CI/KR protection exercise scenarios to increase the level of preparedness?
- How do CI/KR protection efforts relate to initiatives outlined in the jurisdiction's hazard mitigation plan? How do various hazard modeling or ongoing mitigation efforts relate to the CI/KR protection initiatives?
- How will the jurisdiction share best practices, reports, or other output from emergency preparedness activities with CI/KR owners and operators?
- Have CI/KR owners and operators been invited to participate in exercise events, and are CI/KR owners and operators linked to existing warning or response systems?
- What existing education and outreach programs can be leveraged to share information with security partners regarding CI/KR protection?
- Are there other outreach or emergency management programs that should include a CI/KR component?

5A.6 Integrating Federal CI/KR Protection Activities

State-, local-, and tribal-level CI/KR protection programs should complement and draw on Federal efforts to the maximum extent possible to utilize risk management methodologies and avoid duplication of efforts.

State, local, and tribal efforts should consider the adequacy of DHS and SSA guidance and resources for their particular situation. For example:

- Are the existing criteria for risk analysis inclusive of levels of consequence that are of concern to the State or locality, or should the jurisdiction's criteria be expanded to include additional local assets?
- Are the self-assessment tools developed by DHS and the SSAs sufficient, or do these tools need additional tailoring to reflect local conditions?
- Are there additional best practices that should be shared among security partners?
- Are there additional authorities that need to be documented?