

Critical Infrastructure Protection Activities Checklists

Planning Activities

| | |
|--------------------------|--|
| <input type="checkbox"/> | <ul style="list-style-type: none"> <input type="checkbox"/> Develop a consistent approach to critical infrastructure identification. <input type="checkbox"/> Identify critical infrastructure assets and systems. <input type="checkbox"/> Identify dependencies, interdependencies, and key nodes within the jurisdiction. |
| <input type="checkbox"/> | <p>Obtain copies of existing hazard mitigation and emergency operations plans, including:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Critical infrastructure protection plans. <input type="checkbox"/> Hazard mitigation plans (also called hazard plans or mitigation plans). <input type="checkbox"/> Emergency operations plans/Emergency response plans. <input type="checkbox"/> Continuity of operations plans. |
| <input type="checkbox"/> | <p>Either:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Review and update existing plans to ensure that they address critical infrastructure protection; OR <input type="checkbox"/> Collaborate with other governments within the county, region, or State and updating any existing plans and programs to address critical infrastructure within the area of responsibility; OR <input type="checkbox"/> Develop a unique critical infrastructure protection plan and program for the area of responsibility. |
| <input type="checkbox"/> | <p>Ensure that plans identify:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Critical infrastructure protection: <ul style="list-style-type: none"> <input type="checkbox"/> Roles and responsibilities. <input type="checkbox"/> Partners within the jurisdiction. <input type="checkbox"/> Information-sharing mechanisms (both for receiving and for reporting information). <input type="checkbox"/> How critical infrastructure information is used and, if necessary, how it is protected. <input type="checkbox"/> The process used to manage risk to critical infrastructure. <input type="checkbox"/> How the jurisdiction will leverage ongoing emergency preparedness and mitigation activities for critical infrastructure protection. |
| <input type="checkbox"/> | <p>Critical infrastructure or other plans also may identify:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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. <input type="checkbox"/> Whether any roles and responsibilities should be revised, modified, or consolidated to accommodate the unique operating attributes of the jurisdiction. <input type="checkbox"/> How the jurisdiction will maintain operational awareness of the performance of the critical infrastructure protection roles assigned to different offices, agencies, or localities. <input type="checkbox"/> How the jurisdiction will coordinate its critical infrastructure protection roles and responsibilities with other jurisdictions and the Federal Government. <input type="checkbox"/> Unique geographical issues, including transborder concerns. |

Critical Infrastructure Protection Activities Checklists

Partnership Activities

| | |
|--------------------------|--|
| <input type="checkbox"/> | Identify potential critical infrastructure protection partners by leveraging existing public-private partnerships designed to enhance emergency management and community protection and recovery functions. Examples include: <ul style="list-style-type: none"><input type="checkbox"/> Business alliances and partnerships<input type="checkbox"/> Citizen Corps<input type="checkbox"/> State and regional partnerships |
| <input type="checkbox"/> | As appropriate, participate in critical infrastructure sector partnership councils and other forums, including: <ul style="list-style-type: none"><input type="checkbox"/> Sector-specific GCCs and SCCs.<input type="checkbox"/> The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).<input type="checkbox"/> Other critical infrastructure governance and planning efforts relevant to the given jurisdiction. |
| <input type="checkbox"/> | Identify other potential partners and partnership entities: <ul style="list-style-type: none"><input type="checkbox"/> Critical infrastructure owners and operators<input type="checkbox"/> Government partners<ul style="list-style-type: none"><input type="checkbox"/> DHS and other Federal departments, agencies, and offices<input type="checkbox"/> State, local, tribal, and territorial governments<input type="checkbox"/> Critical infrastructure sector partnership councils and other forums (see below)<input type="checkbox"/> Professional associations<input type="checkbox"/> Advisory councils<input type="checkbox"/> Academia and research centers<input type="checkbox"/> Nongovernmental organizations<input type="checkbox"/> Others |
| <input type="checkbox"/> | Invite potential partners to participate. <ul style="list-style-type: none"><input type="checkbox"/> Present the value proposition as necessary.<input type="checkbox"/> Resolve partnership challenges as necessary.<input type="checkbox"/> Identify how and when partners will meet and/or exchange information.<input type="checkbox"/> Establish ground rules for information exchange. For example, identify what information can be shared outside the partnership and what cannot be shared. |
| <input type="checkbox"/> | Establish critical infrastructure partnership goals. Identify specific protection goals that are not currently met under existing hazard mitigation, emergency operations, or other programs. |
| <input type="checkbox"/> | As necessary, coordinate protective activities, preparedness programs, and resource support among local jurisdictions, regional organizations, and private-sector partners. |

Critical Infrastructure Protection Activities Checklists

Information-Sharing Activities

| | |
|--------------------------|--|
| <input type="checkbox"/> | Determine information needs to maintain situational awareness and protect critical infrastructure. Ask: <ul style="list-style-type: none"><input type="checkbox"/> What questions am I trying to answer (who, what, when, where, how)?<input type="checkbox"/> Why do I need this information?<input type="checkbox"/> What am I going to do with this information? |
| <input type="checkbox"/> | Identify information assets (what you currently have or collect) and determine what you can through your own research. |
| <input type="checkbox"/> | Identify other information sources to meet needs. |
| <input type="checkbox"/> | Facilitate the sharing of real-time threat and incident information through partnerships and information-sharing mechanisms. |
| <input type="checkbox"/> | Establish mechanisms for collecting information from critical infrastructure employees and others, identifying: <ul style="list-style-type: none"><input type="checkbox"/> How to encourage participation.<input type="checkbox"/> How to capture reported information.<input type="checkbox"/> How to validate reported information (see below).<input type="checkbox"/> How to forward information. |
| <input type="checkbox"/> | Check collected information for reliability and validity/accuracy. <ul style="list-style-type: none"><input type="checkbox"/> Assess reliability of the source by asking:<ul style="list-style-type: none"><input type="checkbox"/> Does the source have a history of reliability?<input type="checkbox"/> Are there any doubts about the source's competency?<input type="checkbox"/> Are there any doubts about the trustworthiness of the source?<input type="checkbox"/> Was the source in a position to accurately observe the information?<input type="checkbox"/> Double-check the facts. Assess validity/accuracy of the information by asking:<ul style="list-style-type: none"><input type="checkbox"/> Can the information be confirmed by other independent sources?<input type="checkbox"/> Is the information logical?<input type="checkbox"/> Is the information consistent with other information?<input type="checkbox"/> Are there contradictions in the information that need to be addressed? |
| <input type="checkbox"/> | Share critical infrastructure information to enable prioritized protection and restoration of critical public services, facilities, utilities, and functions within the jurisdiction. |

Critical Infrastructure Protection Activities Checklists

Risk Management Activities

| | |
|--------------------------|---|
| <input type="checkbox"/> | <p>Identify threats from adversaries, natural disasters, and technological hazards that could affect critical infrastructure.</p> <ul style="list-style-type: none"><input type="checkbox"/> Obtain threat assessment information concerning terrorism through Federal and other appropriate channels.<input type="checkbox"/> For natural disasters and accidental hazards, use best-available analytic tools and historical data to estimate the likelihood of these events. |
| <input type="checkbox"/> | <p>Assess vulnerabilities and consequences.</p> <ul style="list-style-type: none"><input type="checkbox"/> Assess critical infrastructure vulnerabilities to identified threats.<ul style="list-style-type: none"><input type="checkbox"/> Leverage existing vulnerability assessment programs and tools.<input type="checkbox"/> Incorporate completed vulnerability assessment data.<input type="checkbox"/> Assess potential consequences to critical infrastructure based on identified threats and vulnerabilities.<input type="checkbox"/> Incorporate dependency, interdependency, and other analyses, as needed. |
| <input type="checkbox"/> | <p>Implement protective programs and measures.</p> <ul style="list-style-type: none"><input type="checkbox"/> Identify effective practices based on recognized industry best business practices and standards.<input type="checkbox"/> Leverage existing Federal and other programs. Coordinate with State, regional, and territorial representatives concerning Federal assistance and initiatives. For example:<ul style="list-style-type: none"><input type="checkbox"/> Act as a conduit for requests for Federal assistance when the threat or current situation exceeds the capabilities of the jurisdiction and the private entities resident within it.<input type="checkbox"/> Provide information to owners and operators, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and critical infrastructure funding needs.<input type="checkbox"/> Identify and communicate to DHS requirements from owners and operators for research and development related to critical infrastructure.<input type="checkbox"/> Develop a prioritized implementation plan.<ul style="list-style-type: none"><input type="checkbox"/> Describe assigned tasks with deadlines.<input type="checkbox"/> Provide a means to chart progress in reaching milestones.<input type="checkbox"/> Incorporate implementation into existing plans as needed.<input type="checkbox"/> Implement programs and measures.<ul style="list-style-type: none"><input type="checkbox"/> Establish continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed.<input type="checkbox"/> Provide response and protection, as appropriate, where there are gaps and where local entities lack the resources needed to address those gaps. |

Critical Infrastructure Protection Activities Checklists

Ensuring Continuous Improvement Activities

| | |
|--------------------------|--|
| <input type="checkbox"/> | Participate in education and training offered by government and sector partners as appropriate. <input type="checkbox"/> Arrange for training to be conducted in your jurisdiction as possible. <input type="checkbox"/> Encourage all stakeholders to participate in training sessions. |
| <input type="checkbox"/> | Participate in industry-related and professional or trade association training as needed. <input type="checkbox"/> Arrange for training to be conducted in your jurisdiction as possible. <input type="checkbox"/> Encourage all stakeholders to participate in training sessions. |
| <input type="checkbox"/> | Test and practice protective measures with all stakeholders. <input type="checkbox"/> Conduct red-team testing. <input type="checkbox"/> Practice procedures. |
| <input type="checkbox"/> | Participate in exercises of critical infrastructure protection programs and plans. <input type="checkbox"/> Develop and conduct exercises. <input type="checkbox"/> Include critical infrastructure protection in existing exercises. <input type="checkbox"/> Participate in State and regional exercises. |
| <input type="checkbox"/> | Document lessons learned from predisaster mitigation efforts and testing, exercises, and actual incidents and apply that learning, where applicable, to the critical infrastructure context. |
| <input type="checkbox"/> | Develop implementation plan and take corrective actions. <input type="checkbox"/> Identify additional training needs. <input type="checkbox"/> Identify other needed actions. <input type="checkbox"/> Coordinate with other government and private-sector partners as needed to implement corrective actions. |
| <input type="checkbox"/> | Add or update implementation and other plans as necessary. <input type="checkbox"/> Critical Infrastructure protection plans <input type="checkbox"/> Hazard mitigation plans (also called hazard plans or mitigation plans) <input type="checkbox"/> Emergency operations or response plans <input type="checkbox"/> Continuity of operations plans |