Joint National Priorities for Critical Infrastructure Security and Resilience

In response to risks that threaten essential services and the Nation's safety and prosperity, Presidential Policy Directive-21 (PPD-21) established a national policy to enhance the security and resilience of the Nation's critical infrastructure through proactive and coordinated efforts. Shortly thereafter, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (*NIPP 2013*) furthered ten calls to action to guide the critical infrastructure community[1] toward achieving national and sector goals. Call to Action #1 advocated for the development of joint national priorities to inform resource allocation and decision-making on the part of critical infrastructure partners.

Developed through cross-sector information sharing and collaborative working group sessions, the joint national priorities build upon an evaluation of emerging risks, known capability gaps, resource availability, and best practices. Together, they represent the community-wide distillation of the varied priorities pursued by individual government and industry entities. The joint national priorities are intended to focus partner efforts as they implement activities to accomplish the remaining NIPP calls to action, develop and implement updated Sector-Specific Plans, and pursue related efforts in furtherance of the *NIPP 2013* strategic goals.

While the joint national priorities provide a common focal point for partnership efforts, critical infrastructure partners will continue to share information and implement a variety of security and resilience activities, as appropriate to their unique risk and operating environments.

> *"To guide national efforts and inform decisions, the national council structures will jointly set multi-year priorities and review them annually with input from all levels of the critical infrastructure community."*
>
> *NIPP 2013: Call to Action #1*

The joint national priorities for critical infrastructure security and resilience are:

1. Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure
2. Build Capabilities and Coordination for Enhanced Incident Response and Recovery
3. Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines
4. Enhance Effectiveness in Resilience Decision-Making
5. Share Information To Improve Prevention, Protection, Mitigation, Response, and Recovery Activities

[1] *NIPP 2013 defines the critical infrastructure community as critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; State, local, tribal, and territorial governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so.*

Below is a description of the five joint national priorities. For more information about the joint national priorities, PPD-21, or *NIPP 2013*, please contact NIPP@dhs.gov.

1. Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure

Strengthening risk management of cyber and physical threats and hazards is a national priority, as articulated in PPD-21 and Executive Order (EO) 13636. *NIPP 2013* promotes an integrated, holistic approach to address the increasing reliance of critical infrastructure assets on information and communications technology (ICT) systems and networks. Critical infrastructure partners should use the Framework for Improving Critical Infrastructure Cybersecurity (www.nist.gov/cyberframework) within their organizations and promote its use across sectors and stakeholders. In addition, the critical infrastructure community should explore technological, behavioral, and organizational solutions for managing cyber and physical risks to critical infrastructure.

2. Build Capabilities and Coordination for Enhanced Incident Response and Recovery

The critical infrastructure community should share timely and relevant information during and following incidents to support the rapid restoration of lifeline functions.[2] Critical infrastructure partners should prepare and maintain integrated cyber response and recovery plans to help their organizations manage cyber incidents efficiently and effectively. The critical infrastructure community should improve the tracking and implementation of corrective actions identified through incidents and exercises to inform future planning and response efforts.

3. Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines

Public-private partnerships are the primary mechanism for coordinating and integrating individual partner efforts to manage critical infrastructure risk and share information. A particular priority in the future is to leverage existing national and international partnerships and expand a network of regional and State, local, tribal, and territorial coalitions to strengthen national capacity.

4. Enhance Effectiveness in Resilience Decision-Making

There is broad recognition across the critical infrastructure community of the need to strengthen infrastructure resilience —particularly for infrastructure providing lifeline functions—to increase its ability to withstand and rapidly recover from all hazards under evolving conditions. Effective planning requires evaluation of long-term trends affecting infrastructure risk, such as climate change and increasing reliance on information and communications technology systems. Critical infrastructure partners should consider resilience at each stage of the supply chain and infrastructure lifecycle, including research and development, design, investment, construction, operation, maintenance, repair, and disposal, destruction, or decommissioning. This includes identifying and exploring innovative financing mechanisms to encourage investments that enhance all-hazard resilience.

5. Share Information To Improve Prevention, Protection, Mitigation, Response, and Recovery Activities

Sharing timely, relevant information and intelligence promotes awareness of threats and hazards, enabling the implementation of measures to mitigate risk. Collaborative efforts in government and industry focus on determining priorities for analysis in the context of the critical infrastructure operating environment, establishing and using reliable and appropriate means of dissemination across and within sectors, and providing feedback for continuous improvement. The overall goal of these efforts is an information-sharing culture based on the "need to share" and "responsibility to provide."

---

[2] *NIPP 2013 identifies four lifeline functions on which all critical infrastructure sectors rely, to include energy, communications, transportation, and water.*