



**Homeland  
Security**

# Critical Infrastructure Security and Resilience Month

November is Critical Infrastructure Security and Resilience Month, which recognizes the important role critical infrastructure plays in our Nation's way of life and why it is important to expand and reinforce critical infrastructure security and resilience.

## What Critical Infrastructure Means To You

The Nation's critical infrastructure provides essential services that underpin American society and sustain the American way of life. Critical infrastructure supports the power we use in our homes, the water we drink, the transportation systems that get us from place to place, the bridges that connect us, and the communication systems we rely on to stay in touch with friends and family.

Securing critical infrastructure and ensuring its resilience is a shared responsibility of Federal, State, local, tribal, territorial, and private sector partners, as well as individual citizens. Just as we all rely on critical infrastructure, we must all play an active role in keeping it strong, secure, and resilient.

Critical Infrastructure Security and Resilience Month focuses on building awareness and understanding of the importance of critical infrastructure to America's national security and economic prosperity, as well as reaffirming the commitment to keep our critical infrastructure and our communities safe and secure. This requires a nationwide effort, with partners working together toward a common goal.

## How You Can Get Involved

- Read the Presidential Proclamation.
- Share stories and information about your efforts in support of infrastructure security and resilience with your customers, constituents, partners, residents, and employees through newsletters, websites, emails, blog posts, and tweets.
- Reinforce the role your organization/office plays in infrastructure security and resilience by incorporating references to Critical Infrastructure Security and Resilience Month in speaking engagements and events.
- Follow [@DHSgov](https://twitter.com/DHSgov) on Twitter, and post infrastructure security and resilience efforts, tips, news, and resources on social media sites using #infrastructure.
- Download the Critical Infrastructure Security and Resilience Month toolkit at <http://www.dhs.gov/publication/cisr-month-toolkit> to help spread the word.

Americans can do their part at home, at work, and in their local communities by being prepared for all hazards, reporting suspicious activities, and learning more about critical infrastructure security and resilience.

## What Is Critical Infrastructure?

Protecting and promoting the continuity of our Nation's critical infrastructure is essential to our security, public health and safety, and economic vitality. Critical infrastructure refers to the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on our Nation's way of life.



Critical infrastructure is increasingly at risk from a variety of hazards—including climate change and extreme weather, aging and failing infrastructure components, cyber threats, pandemics, and acts of terrorism. These threats have evolved over the years. In particular, physical and cyber infrastructure have grown inextricably linked, meaning both cyber and physical measures are required to guard against the full array of threats. Growing interdependencies among infrastructure sectors and the lifeline functions we all rely on also impact the management of national critical infrastructure risk. Understanding and mitigating these risks is a key element of our national security, resilience, and economic prosperity.

## The Role of IP

The Department of Homeland Security's National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) leads the coordinated national effort to manage risks to our Nation's critical infrastructure. NPPD leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. IP focuses on protecting critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

IP leads this national effort by working with critical infrastructure partners to achieve the aims articulated in the National Infrastructure Protection Plan (NIPP). The NIPP envisions critical infrastructure that is secure and able to withstand and rapidly recover from all hazards. It focuses on a set of lifeline functions—communications, energy, transportation, and water management—to support preparedness and continuity of operations.

## The Critical Role of Partnerships

IP works with other DHS components; Federal, State, local, tribal, and territorial agencies; and the private sector to address critical infrastructure national security imperatives to:

- Secure vital assets.
- Ensure continuity of operations.
- Prepare for response to and recovery from all-hazards events.

To accomplish this mission of ensuring critical infrastructure security and resilience, DHS relies on support from partners and stakeholders. Public-private partnerships, in particular, are vital to this effort. Because the majority of our national critical infrastructure is owned and operated by private companies, both the government and private sector have a common incentive to reduce the risks of disruptions to critical infrastructure. Strengthening public-private partnerships focused on critical infrastructure protection is both a national security and business imperative.

The NIPP calls on partners to further existing efforts to manage risk by developing joint priorities, empowering local and regional partners, engaging in collective actions, and leveraging incentives to progress toward a national focus on security and resilience. It also emphasizes the need for innovative risk management to enable informed decision making based on identified dependencies, interdependencies, and potential cascading effects. IP supports critical infrastructure partners in achieving these aims in a number of ways, including:

- **Information Sharing:** IP facilitates information sharing across infrastructure stakeholders. This includes sharing sensitive information regarding critical infrastructure, threats, and best practices to strengthen owners' and operators' decision-making capabilities.
- **Training & Education:** IP facilitates collaborative exercises and provides training materials, courses, and consultation to sector partners across the Nation and internationally, augmenting the critical infrastructure community's awareness, preparedness, and response capabilities.
- **Partnerships:** IP facilitates partnerships across Federal, State, local, tribal, and territorial entities and the private sector that enable comprehensive response and collaborative engagement throughout the critical infrastructure community.
- **Assessments, Analysis, & Regulatory Compliance:** IP supports critical infrastructure partners in achieving regulatory compliance and managing risk based on threat, vulnerability, and potential consequence assessments. Risk assessments and analysis helps identify requirements for security programs and resiliency strategies.