Homeland Security

Office of Infrastructure Protection

What is Critical Infrastructure?

Critical infrastructure plays a vital role in our Nation's security, public health and safety, and economic vitality every day. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, the bridges that connect us, and the communication systems we rely on to stay in touch with friends and family. More broadly, 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, presenting ever-changing challenges. 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. Furthermore, growing interdependencies between infrastructure sectors and the lifeline functions we all rely on increase the possibility of cascading effects if a single sector is disrupted. Understanding and mitigating these risks is a key element of our national security, resilience, and economic prosperity.

Examples of critical infrastructure
(Courtesy of DHS)

The Role of the Office of Infrastructure Protection

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. IP acts on behalf of the Secretary of Homeland Security, implementing the national critical infrastructure protection responsibilities set forth in Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. PPD-21 and Executive Order (EO) 13636 on Critical Infrastructure Cybersecurity reaffirmed the essential mission of IP in driving resilience across the Nation's infrastructure.

IP's efforts support the broader mission of the Department and the specific aims of NPPD, which 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, which includes private sector owners, operators, and employees; State, local, tribal, and territorial officials; and other Federal agencies.

IP leads this national effort by working with critical infrastructure partners to achieve the aims articulated in the National Infrastructure Protection Plan (NIPP), in conjunction with national preparedness policy articulated in PPD-8: National Preparedness. The NIPP envisions critical infrastructure that is secure, 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

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. Public-private partnerships, in particular, are vital to this effort as DHS relies on support from partners and stakeholders to accomplish its mission of ensuring critical infrastructure security and resilience. To this end, 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

These imperatives are supported by the aims of the NIPP, which calls on partners to further existing efforts to manage risk by developing joint priorities, empowering local and regional partners, engaging in collective actions, leveraging incentives to progress toward a national focus on security and resilience, and enabling 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:

Owner-Operators
Customer Relations
Operations
Investment
State, Local, Regional
Public Safety
Law Enforcement
Utility Regulation
NIPP 2013
Federal Government
National Policy
Information Sharing
Coordination
NGOs
Trusted Relationships
Community Building
Research

Critical infrastructure partners as described in the NIPP (Courtesy of DHS)

- **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 help identify requirements for security programs and resiliency strategies.