



The Internet underlies nearly every aspect of our everyday lives and helps form our critical infrastructure, which keeps crucial systems like electricity, transportation and communications up and running. It's important to protect this vast network and properly secure the systems that connect to the Internet. October 31 will emphasize the importance of critical infrastructure and highlight the roles the public can play in keeping it secure. On this last day of October, the transition to Critical Infrastructure Security and Resilience Month in November begins.



National Cyber Security Awareness Month

Building Resilience in Critical Systems

About the Significance of Critical Infrastructure...

What is critical infrastructure?

The Nation's critical infrastructure provides the essential services that underpin American society. Ensuring delivery of essential services and functions is important to sustaining the American way of life.

We know it as the power we use in our homes, the water we drink, the transportation that moves us, the bridges that connect us, and the communication systems we rely on to stay in touch with friends and family.

America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards, including cyber-attacks. Critical infrastructure security and resilience requires a clear understanding of the risks we face and a whole-of-community effort that involves partnership between public, private, and non-profit sectors.

Who is the critical infrastructure community?

Just as we all rely on critical infrastructure, we all play a role in keeping it strong, secure, and resilient. Securing and making critical infrastructure resilient is a shared responsibility—shared by Federal, State, local, tribal, and territorial governments; private companies; and individual citizens.

Are there challenges facing critical infrastructure today as a result of cyber interdependencies?

Critical infrastructure is highly interconnected and any single system may rely on other critical infrastructure to be running at normal operations. In particular, nearly all critical infrastructure relies heavily on network and other cyber support to operate essential systems. However, it is important to understand how critical infrastructure relies on secure cyber systems, but also how to protect our critical infrastructure against cyber-attacks.



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

Why is it important to focus on the critical infrastructure needs of the country?

The vast majority of our Nation's critical infrastructure is privately owned and operated, and both the government and private sector have a shared responsibility to prevent and reduce the risks of disruptions to critical infrastructure. Investments in infrastructure protection are crucial to the resilience of the public and private sectors. Together, public and private efforts to strengthen critical infrastructure show a correlated return on investment, helping the public sector enhance security and rapidly respond to and recover from all-hazards events and the private sector restore business operations and minimize losses in the face of such an event.

What are some of the challenges facing critical infrastructure today?

Threats to the Nation's critical infrastructure include extreme weather, aging infrastructure, cyber threats, and acts of terrorism. The evolving nature of the threat to critical infrastructure—as well as the maturation of our work and partnership with the private sector—has necessitated a shift from a focus on asset protection to one on overarching system resilience from all threats and hazards.

Help the authorities fight cybercrime:

The Department of Homeland Security is committed to leading the national effort to make infrastructure secure and resilient in the face of all hazards, including cyber vulnerabilities. Through Critical Infrastructure Security and Resilience Month, DHS is promoting a shared awareness and understanding across the critical infrastructure community of the diverse hazards affecting resilience and ensuring DHS partners have access to the resources and tools needed to inform decision making to address cyber related challenges. Visit www.dhs.gov/cybersecurity for tools and tips on cybersecurity.

Content provided by dhs.gov