



**Homeland
Security**

**Executive Order (EO) 13636 Improving Critical
Infrastructure Cybersecurity**

**Presidential Policy Directive (PPD)-21 Critical
Infrastructure Security and Resilience**

Background

The Department of Homeland Security (DHS) leads the Federal government's efforts to secure our Nation's critical infrastructure by working with owners and operators to prepare for, prevent, mitigate, and respond to threats. While DHS plays a central role, the Department cannot do this work alone. Public private partnerships are essential. It is through partnerships where the Department continues to see new value and positive impact in mitigating and rapidly responding to crises.

Facing threats to our Nation from cyber attacks that could disrupt our power, water, communication and other critical systems, the President issued the *Executive Order (EO) on Improving Critical Infrastructure Cybersecurity* and *Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience*. These policies reinforce the need for holistic thinking about security and risk management. Implementation of the EO and PPD will drive action toward system and network security and resiliency, and will also enhance the efficiency and effectiveness of the U.S. government's work to secure critical infrastructure and make it more resilient.

Executive Order 13636: Improving Critical Infrastructure Cybersecurity directs the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
- Explore the use of existing regulation to promote cyber security

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
- Understand the cascading consequences of infrastructure failures
- Evaluate and mature the public-private partnership
- Update the National Infrastructure Protection Plan
- Develop comprehensive research and development plan

Learn more about [the Department's efforts to strengthen and secure the Nation's critical infrastructure.](#)