THE WHITE HOUSE

Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS

February 12, 2013

EMBARGOED: FACT SHEET: PRESIDENTIAL POLICY DIRECTIVE ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

To complement the Cyber Security Executive Order issued today, the Administration is also issuing a Presidential Policy Directive (PPD) on critical infrastructure security and resilience that updates the national approach from Homeland Security Presidential Directive 7, issued in 2003, to adjust to the new risk environment, key lessons learned, and drive toward enhanced capabilities.

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary for us to strengthen and maintain secure, functioning, and resilient critical infrastructure – including the assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical and cyber spaces, and governance constructs that involve varied authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

While there has been extensive work done to enhance both the physical and cyber security and resilience of critical infrastructure, this PPD will create a stronger alliance between these two intertwined components. The ability to leverage and integrate successes in both of these fields is crucial to the enhancement of our Nation's security and resilience.

Three strategic imperatives drive the Federal approach to strengthen critical infrastructure security and resilience:

- Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;

- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and

- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

Accomplishment of these imperatives will be through the successful completion of six key deliverables:

- Development of a description of the functional relationships within the Department of Homeland Security and across the Federal Government related to critical infrastructure security and resilience within 120 days.

- Completion of an assessment of the existing public-private partnership model and recommended options for improving the partnership within 150 days.

- Identification of baseline data and systems requirements for the Federal Government to enable efficient information exchange within 180 days.

- Development of a situational awareness capability for critical infrastructure within 240 days.

- Update the National Infrastructure Protection Plan within 240 days.

- Completion of a national critical infrastructure security and resilience research and development plan within 2 years.

###