Fact Sheet: Executive Order on Cybersecurity / Presidential Policy Directive on Critical Infrastructure Security and Resilience

Release Date: February 13, 2013

Critical infrastructure – both physical and cyber – is the backbone of America's national security and economic prosperity. The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multi-national ownership), interdependent functions and systems in both physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure faces a variety of risks to its security and ability to function, including manmade acts of terror, extreme weather events, other natural disasters and cyber attacks.

Our country's reliance on cyber systems to run everything from power plants to pipelines and hospitals to highways has increased dramatically, and our infrastructure is more physically and digitally interconnected than ever. Yet for all the advantages interconnectivity offers, critical infrastructure is also increasingly vulnerable to attack from an array of cyber threats.

It is imperative that we, as a country, take more action to strengthen our national policy on critical infrastructure security and resilience, and that includes measures to strengthen cybersecurity. Because the majority of our critical infrastructure is owned and operated by private companies, the public and private sectors have a shared responsibility to reduce the risks to critical infrastructure through a stronger partnership.

In May 2009, President Obama declared our digital infrastructure a strategic national asset, recognizing that protecting the networks and computers that deliver essential services such as our oil and gas, power, and water is a national security priority. President Obama is committed to doing everything in his power to protect these systems from cyber threats. In May 2011, the Obama Administration sent Congress a cybersecurity legislative proposal. Today the President signed an Executive Order (EO) on Cybersecurity and a Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience. These actions will strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

Together, the EO and PPD create an opportunity to reinforce the need for holistic thinking about security risk management and drive action toward a whole of community approach to security and resilience. The documents also create leverage to dramatically enhance the efficiency and effectiveness of the U.S. Government's efforts to protect critical infrastructure.

The need to improve cybersecurity is an area of significant bipartisan agreement, and the Executive Order issued today incorporates approaches supported by business leaders, researchers, and members of Congress for how to effectively achieve that shared goal. This Executive Order is a down payment on strengthening our critical infrastructure, but the nation still requires cybersecurity legislation in order to update the government's authorities to address this urgent threat.

The Executive Order strengthens the U.S. Government's partnership with the private sector to address these threats through:

- **New information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies.** The Executive Order requires Federal agencies to produce unclassified reports of threats to relevant U.S. companies and requires the reports to be shared in a timely manner. The Order also expands the Enhanced Cybersecurity Services program beyond the Defense Industrial Base, allowing companies in other sectors to participate.
- **The development of a Cybersecurity Framework.** The Executive Order directs the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. NIST will work collaboratively with industry to develop the framework and will incorporate existing international standards, practices, and procedures wherever possible. To promote technical innovation, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services.

The Executive Order also:

- **Establishes a voluntary program to promote the adoption of the Framework.** The Department of Homeland Security will work with Sector-Specific Agencies and the Sector Coordinating Councils that represent industry to develop a program to assist companies with implementing the framework and to identify incentives for adoption of the framework. Additionally, Federal executive branch civilian agencies will adopt the framework to enhance the protection of their systems.
- **Calls for a review of existing cybersecurity regulation.** Some sectors – but not all – of our most critical infrastructure already fall under existing cybersecurity regulation. For those sectors, regulatory agencies will review the Cybersecurity Framework and determine if existing regulatory requirements provide sufficient cybersecurity. If the existing regulations are insufficient, then agencies will propose new, cost-effective regulations based upon the Cybersecurity Framework. Regulatory agencies will use their existing processes to consult with their regulated companies to develop and propose any new regulations.
- **Includes strong privacy and civil liberties protections based on the Fair Information Practice Principles.** Agencies are required to incorporate privacy and civil liberties safeguards in their cybersecurity activities under this order. Those safeguards will be based upon the Fair Information Practice Principles (FIPPs) and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies will conduct regular assessments of privacy and civil liberties impacts of their activities and such assessments will be made public.

By working together, the critical infrastructure community and the Federal government have done remarkable work over the last ten years in creating new tools and delivering new services that improve how the public and private sector work together to protect our critical infrastructure. To complement the Cyber Security Executive Order, the Administration is issuing a Presidential Policy Directive 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. Specifically, the PPD:

- **Directs the government to identify the functional relationships across the government** related to critical infrastructure and work to improve the effectiveness of the existing public-private partnership with owners and operators and state, local, tribal and territorial partners in both the physical and cyber space.
- **Directs the government to develop an efficient situational awareness capability** that addresses both the physical and cyber implications of an incident and ensures further integration and awareness throughout the government and enables responsible sharing of the implications with stakeholders.
- **Directs the government to address other information sharing priorities**, including speeding up the information flow to respond to the changing risk environment, as well as strengthening our capability to understand and share information about how well infrastructure systems are functioning and the consequences of infrastructure failures.
- **Calls for a comprehensive research and development plan for critical infrastructure to guide the government's effort to enhance and encourage** market-based innovation.

###

Review Date: *February 13, 2013*