The White House

Office of the Press Secretary

For Immediate Release February 12, 2013

Executive Order on Improving Critical Infrastructure Cybersecurity

Today, President Obama signed an Executive Order to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with our industry partners.

- **Defense Industrial Base Information Sharing Program Now Open to Other Sectors**: The Order expands the voluntary Enhanced Cybersecurity Services program, enabling near real time sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts.

- **NIST to Lead Development of Cybersecurity Framework**: NIST will work collaboratively with critical infrastructure stakeholders to develop the framework relying on existing international standards, practices, and procedures that have proven to be effective.

Partnering with Industry to Protect Our Most Critical Assets from Cyber Attack

Today's new Executive Order was developed in tandem with the Presidential Policy Directive on Critical Infrastructure Security and Resilience also released today. The Executive Order strengthens the U.S. Government's partnership with critical infrastructure owners and operators to address cyber 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 U.S. companies and requires the reports to be shared in a timely manner. The Order also expands the Enhanced Cybersecurity Services program, enabling near real time sharing of cyber threat information to assist participating critical infrastructure companies in their cyber protection efforts.

- **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 of cybersecurity practices to reduce cyber risks to critical infrastructure. NIST will work collaboratively with industry to develop the framework, relying on existing international standards, practices, and procedures that have proven to be effective. To enable 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:

- **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 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.

- **Establishes a voluntary program to promote the adoption of the Cybersecurity Framework**. The Department of Homeland Security will work with Sector-Specific Agencies like the Department of Energy and the Sector Coordinating Councils that represent industry to develop a program to assist companies with implementing the Cybersecurity Framework and to identify incentives for adoption.

- **Calls for a review of existing cybersecurity regulation**. Regulatory agencies will use the Cybersecurity Framework to assess their cybersecurity regulations, determine if existing requirements are sufficient, and whether any existing regulations can be eliminated as no longer effective. If the existing regulations are ineffective or insufficient, agencies will propose new, cost-effective regulations based upon the Cybersecurity Framework and in consultation with their regulated companies. Independent regulatory agencies are encouraged to leverage the Cybersecurity Framework to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Building on Progress

In May of 2009, President Obama declared our digital infrastructure a strategic national asset and made protecting this infrastructure a national priority. As part of this effort, the Obama Administration has:

- **Created the National Cybersecurity & Communications Integration Center**: The NCCIC is a 24-hour, DHS-led coordinated watch and warning center that improves our nation's ability to address threats and incidents affecting critical infrastructure, the Internet, and cyberspace.

- **Issued the National Strategy for Trusted Identities in Cyberspace**: The NSTIC and its programs are creating alternatives to passwords for online services that are more convenient, secure, and privacy enhancing.

- **Submitted to Congress Comprehensive Cybersecurity Legislation**: The Administration continues to believe that legislation is needed to fully address this threat. Existing laws do not permit the government to do all that is necessary to better protect our country. The Executive Order ensures that federal agencies and departments take steps to secure our critical infrastructure from cyber attack, as a down-payment on expected further legislative action.