U.S. DEPARTMENT OF ENERGY

Office of Electricity Delivery and Energy Reliability (OE)

Infrastructure Security and Energy Restoration (ISER)

Energy Emergency Preparedness Quarterly

VOLUME 2, ISSUE 2 APRIL 15, 2013

New Critical Infrastructure Cybersecurity Executive Order

The continued growth of cyber threats against our critical infrastructure (CI) is one of the most significant national security issues facing the Nation. In an effort to improve cybersecurity and enhance the security and resiliency of the Nation's CI, on February 12, 2013, President Obama released Executive Order 13636 - Improving Critical Infrastructure Cybersecurity (E.O. 13636). Critical infrastructure refers to those systems and assets, either physical or virtual, which are so vital to the United States that their incapacitation or destruction would have a debilitating impact on the security, national economic security, national public health or safety, or a combination thereof. (P.L. 107–296). Through increased partnership and enhanced information sharing with CI owners and operators, E. O. 13636 supports the growth and preservation of an efficient, innovative, and economically prosperous cyber environment without compromising safety, security, business confidentiality, or privacy and civil liberties.

An Overview of Executive Order 13636 — What it Does

- Requires the development of processes to ensure unclassified reports identifying a specific U.S. cyber target are rapidly produced and disseminated to targeted entities while also protecting intelligence and law enforcement sources, operations, and investigations.
- Expands the voluntary Enhanced Cybersecurity Services (ECS) program to all CI sectors by providing classified Government information and cyber threats to CI companies or eligible commercial security service providers.
- Expedites processing of security clearances for appropriate personnel employed by CI owners and operators.
- Expands programs that place private sector subject matter experts into Federal service.
- Requires the integration of privacy and civil liberties protections into all cyber activities.
- Provides technical assistance to Sector-Specific Agencies to develop cybersecurity workforces and cyber programs.
- Coordinates CI cybersecurity improvements through the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; Sector-Specific Agencies, CI owners and operators; regulatory institutions, and other relevant entities.
- Directs the National Institute of Standards and Technology (NIST) to lead the development of a technology-neutral framework to reduce cyber risks to CI which aligns policy, business, and technological approaches and incorporates industry best practices in a prioritized set of methodologies, procedures, and processes.
- Supports adoption of the framework through a voluntary CI cybersecurity program.
- Incentivizes program participation and gauges if incentives can be provided under existing laws or if new legislation is required.
- Identifies highest risk CI in which a cybersecurity incident may result in catastrophic regional or national effects, and confidentially notifies those CI owners and operators.

Deputy Assistant Secretary ISER

William N. Bryan

Director, Preparedness and Response ISER

Stewart Cedres

DOE Provides Support for the Presidential Inauguration

In accordance with the Presidential Threat Protection Act of 2000 (P.L. 106-544), the Secretary of the Department of Homeland Security (DHS) is responsible for designating major events of national significance as National Special Security Events (NSSE) on behalf of the President of the United States. The determination to designate an event as a NSSE is based upon a number of factors including anticipated attendance by U.S. officials and visiting and foreign dignitaries, and the size and significance of the event. Events designated as NSSEs include major summits of world leaders and meetings of international organizations held in the United States, national presidential nominating conventions, presidential inaugurations, and major sports events. The U.S. Secret Service (USSS) is the designated lead Federal

agency responsible for developing, planning, coordinating, exercising, and implementing security operations for NSSEs. The numerous and complex challenges unique to these events necessitates extensive planning and operational coordination by Federal, state, regional, local, private, and non-governmental organizations well in advance of the event.

For the 2013 Presidential Inauguration, a designated NSSE, the USSS relied upon an experienced team from the Department of Energy (DOE) to help manage energy issues and address potential disruptions or threats to the energy infrastructure in the region supporting the event. The DOE team, led by Bob Reed, was involved in pre-event planning and coordination, developed specialized reports and analytical products, and provided subject matter expertise and on-site support and guidance throughout the event.

In support of the inauguration, the team participated in meetings with the Critical Infrastructure Subcommittee, one of many functional groups established to efficiently manage specific needs during the event. Team members also furnished the USSS with specialized reports which described and mapped regional energy infrastructure and provided a detailed operational assessment, including capacity and interdependencies, for each asset. The team worked with local utilities and the regional transmission organization to coordinate a series of assessments of critical substations with the utility and the USSS. They staffed the Multi Agency Communication Center (MACC), a 24-hour communication and coordination facility for Federal agencies and law enforcement officers, and the Critical Infrastructure Resource Center (CIRC), a USSS center comprised of utilities, critical infrastructure owners, and select federal partners.

The DOE team's dedication and professionalism have made them a go-to NSSE resource for the USSS, with the team again lending their support in late April for the dedication of the George W. Bush Library and Museum in Dallas, an event that President Obama and the four living former U.S. Presidents also attended.

Presidential Policy Directive 21 is Released

Presidential Policy Directive 21 (PPD-21) - Critical Infrastructure Security and Resilience, was released in February, revoking Homeland Security Presidential Directive 7 (HSPD-7) - Critical Infrastructure Identification, Prioritization, and Protection. PPD-21 expands the Nation's primary critical infrastructure (CI) protection focus from protection against terrorist attacks to an all-hazards approach, which also encompasses natural disasters, pandemics, and cyber attacks. PPD-21 reaffirms the Department of Energy as the energy Sector-Specific Agency (SSA), and identifies energy and communications systems as especially critical sectors due to their importance across every CI sector. The directive is also integrated with the National Preparedness System across each of the five mission areas: prevention, protection, mitigation, response, and recovery.

Through PPD-21, the Federal approach for strengthening CI security and resilience is structured around three strategic imperatives: 1.) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen CI security and resilience; 2.) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and 3.) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

The Secretary of the Department of Homeland Security (DHS), along with the SSAs, other Federal departments and agencies, state, local, tribal, and territorial entities, and CI owners and operators, as applicable, will implement PPD-21 through the following key deliverables:

- Development of a comprehensive description of CI security and resilience functional relationships within DHS and across the Federal government to serve as a roadmap for CI security and resilience for both physical and cyber threats.
- Evaluation of the existing Public-Private Partnership Model with recommendations for improving efficacy of physical and cyber partnerships by eliminating duplication of efforts and enhancing information sharing.
- Identification of the baseline data and systems requirements for the Federal government to facilitate information sharing, address interoperability, availability and accessibility of data, and protect privacy and civil liberties.
- Development of a near real-time physical and cyber CI situational awareness capability with threat and vulnerability information, and infrastructure status and potential cascading effects.
- Update of the National Infrastructure Protection Plan by identifying a risk management framework, and methods to prioritize CI and align to the National Preparedness System.
- Development of a National Critical Infrastructure Security and Resilience R&D Plan to help guide and prioritize future R&D investments and requirements.