U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

February 1, 2011

The Department of Energy Launches Cyber Security Initiative

Collaborative effort will develop a risk management process guideline

WASHINGTON, DC - The Department of Energy is launching an initiative to enhance cyber security on the electric grid. The initiative, led by the Department's Office of Electricity Delivery and Energy Reliability (OE), the National Institute of Standards and Technology, and the North American Electric Reliability Corporation, will be an open collaboration with representatives from across the public and private sectors to develop a cyber security risk management process guideline for the electric sector.

Traditional cyber security approaches for electric utilities are segmented, with different approaches for control systems and information systems. This has resulted in cyber security requirements that are overly restrictive in some cases, and not restrictive enough in others. At best, requirements are overlapping, but more often result in gaps in cyber security coverage. A common approach is needed to address the unique cyber security risks that a nation-wide smart grid will pose.

"Cyber security is vital to the development of a modern electric grid," said OE Assistant Secretary Patricia Hoffman, "We recognize that each utility faces different risks; now we need to provide them with standard, adaptable solutions to manage those risks."

"Electric sector asset owners in North America are a vast and diverse group of individual companies," said Gerry Cauley, CEO of the North American Electric Reliability Corporation. "This collaborative approach to develop security guidelines for managing risk across the electric grid is an innovative process that addresses the diversity and will provide greater benefits to industry."

"Effectively managing cyber security risk in the electric grid will require utilities to have an integrated approach across missions, business processes and the control systems and information systems that support those processes", said George Arnold, NIST's National Coordinator for Smart Grid Interoperability. "Placing cyber security into the broader organizational context of achieving mission and business success will enable utilities to make strategic risk management decisions."

The leadership team has invited stakeholders from across the electric sector to participate, including representatives from the Federal Energy Regulatory Commission, the Department of Homeland Security, and both publicly and privately-owned utilities. The group will develop a risk management process guideline that provides utilities a flexible, fundamental approach to managing cyber security risks through a three-tiered approach, addressing risks at the (i) *organization* level; (ii) *mission/ business process* level; and (iii) *information system* level. This process will allow a utility to better understand its risks, assess the severity, and allocate resources more efficiently to manage them.

A draft guideline will be made available for public review and comment before it is finalized and issued.

###

For more information, visit DOE's Office of Electricity Delivery and Energy Reliability website.

Media contact(s):

(202) 586-4940