**Department of Energy**
Washington, DC 20585

March 19, 2012

Chad Whiteman
Policy Analyst
Office of Information and Regulatory Affairs
Office of Management and Budget
Executive Office of the President

Mr. Whiteman,

The Department of Energy would like to request an emergency ICR, as well as a FRN as soon as possible for a short a time as possible (15 days). Below I have included the purpose of the pilot, DOE's requirements for creating the initiative, and a justification for the emergency request. I have also included a draft of the FRN.

**Purpose of Collection:** To gather feedback from industry on the validity of a draft maturity model developed through a public-private collaborative effort. The objective of the maturity model is to provide the information needed for owners and operators of the nation's electric utilities, as well as the government agencies supporting the sector, to understand what capabilities and competencies will allow the sector to defend itself, and inform investment decisions.

**DOE Requirements:** DOE is exercising its authority to collect information, as granted in the Department of Energy Organization Act, 91 Stat. 565; 42 U.S.C. $7101, and required by Homeland Security Presidential Directive 7. DOE is working at the request of the White House and in partnership with DHS and sector entities to provide the information needed and requested by the sector to increase security and the resiliency of the Nation's energy grid in light of increasing cyber attacks.

**Emergency Justification:** "Protecting the electric system from cyber threats and ensuring its resilience are vital to our national security and economic well-being. This is exactly why cybersecurity is one of four key themes in the White House's Policy Framework for a 21st Century Grid."[1] The constant escalation of cyber threats against the nation, and in particular critical infrastructure, has created a significant need for information on how owners and operators can invest in and learn from best practices to protect themselves from threats and to increase the resiliency of their systems. Critical Infrastructure Protection is a White House National Security priority. The Electric Sector Cybersecurity Risk Management Maturity Initiative is under development with public and private sector partners to provide this capability to the sector as soon as possible. The initiative pilot, for which the emergency ICR is being

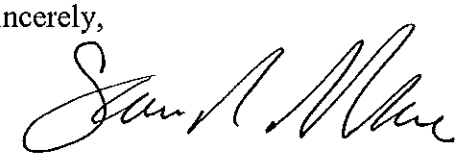
[1] Protecting the Nation's Electric Grid from Cyber Threats, http://www.whitehouse.gov/blog/2012/01/09/protecting-nation-s-electric-grid-cyber-threats

Printed with soy ink on recycled paper

requested, will test and validate the model and assessment tool so that it can be revised and improved. The results of the pilot can then be provided to the sector as whole to help them immediately begin to identify areas of their systems and processes where investments or resources can be made or reconfigured to bolster the security of their systems further protecting the reliability of the electric grid from disruptive or costly cyber threats.

If there is anything I or my organization can do, please feel free to contact me at 202-586-1283 or samara.moore@hq.doe.gov.

Sincerely,



Samara Moore
Sr. IT and Cyber Security Advisor
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy