Department of Water and Power the City of Los Angeles

ANTONIO R. VILLARAIGOSA
*Mayor*

Commission
THOMAS S. SAYLES, *President*
ERIC HOLOMAN, *Vice President*
RICHARD F. MOSS
CHRISTINA E. NOONAN
JONATHAN PARFREY
BARBARA E. MOSCHOS, *Secretary*

RONALD O. NICHOLS
*General Manager*

April 29, 2013

Office of Policy Analysis and Development
National Telecommunications and Information Administration (NTIA)
United States Department of Commerce
1401 Constitution Avenue, N.W. Room 4726
Washington, DC 20230

Subject: Incentives to Adopt Improved Cybersecurity Practices

The Los Angeles Department of Water and Power (LADWP) appreciates the opportunity to respond to the Notice of Inquiry (NOI) issued by the National Telecommunications and Information Administration, and published in the Federal Register on March 28, 2013.

LADWP is the largest municipal water and power utility in the nation, and was established more than 100 years ago. LADWP delivers reliable, safe water and electricity to approximately 3.8 million residents and businesses in the City of Los Angeles.

LADWP has developed and implemented a robust cyber security program pursuant to the North-American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. LADWP ensures that it continuously remains in compliance with all aspects of the CIP Standards, and believes that these standards establish an important baseline for properly securing Bulk Power System assets.

LADWP welcomes the opportunity to provide comments on potential incentives "that may be necessary to encourage" participation in the voluntary Cybersecurity Framework (Framework) being developed by the National Institute of Standards and Technology (NIST), effort that has been directed in the President's Executive Order



111 North Hope Street, Los Angeles, California 90012-2607 *Mailing address:* Box 51111, Los Angeles 90051-5700
*Telephone:* (213) 367-4211 *Cable address:* DEWAPOLA

13636[1] (Executive Order). LADWP believes that this voluntary Framework could be established to complement existing NERC CIP standards.

From LADWP's perspective, incentives will be an important factor in a company's decision-making process when deciding as to whether to adopt and participate in the Cybersecurity Framework, to the extent that those incentives and overall system benefits outweigh the additional costs of implementation. As a public power entity with a public service mission to provide reliable, competitive and environmentally responsible energy to its owners (the residents of Los Angeles), and with rates that are set by its Board and City Council, it is important that incentives are in place so that the costs are not all shifted to its ratepayers, and to aid in finding a proper balance between benefits and costs.

Incentives

LADWP finds the following incentives[2] as establishing a good baseline to motivate owners of cyber-infrastructure to join a reasonable, voluntary Cybersecurity Framework:

- Grants and Low-Interest Loans: Providing federal funding for investing in cybersecurity infrastructure and services for cyber assets owners and operators. For example, these grants/loans could be used to offset the cost of vulnerability assessments or emergency response plans. In the alternative, the federal government could provide grants for joining the Framework;

- Liability: Providing safe-harbor protection from claims arising from cybersecurity breaches, when the entity has implemented strong cybersecurity measures, contingent upon reasonable efforts to conform to the Framework requirements;

- Insurance: Providing incentives and/or federal insurance programs to help underwrite insurance programs to cover potential damages during cybersecurity breaches;

- Information Sharing: Ensuring that Framework participants are provided with relevant real-time cyber threat information, and privacy of entities and individuals are protected as required by law;

- Expedited Security Clearances: Establishing procedures to expedite the provision of security clearances to appropriate personnel employed by critical infrastructure owners and operators under the Framework;

- Prioritize Assistance: Ensuring Framework owners/operators receive prioritized assistance from the federal government during cybersecurity breaches; providing

[1] "Executive Order 13636 – Improving Critical Infrastructure Cybersecurity" 78 FR 11739 (February 19, 2013)

2 As generally discussed by the Cross Sector Cyber Security Working Group – Incentives Subgroup Incentive Recommendations (April 2009).

preferred on-location training on cybersecurity "best practices" (e.g. from appropriate Homeland Security Response Teams); and making available vulnerability assessment tools.

Barriers to Cybersecurity Framework Implementation

One of the main barriers for companies to implement measures beyond those required by current NERC CIP standards is human resources availability. Proper incentives may assist in balancing more effectively costs and benefits, and thus, possibly helping overcome this obstacle.

Effectiveness Determination

Effectiveness of these incentives in bringing about stronger cyber-breach protections may be determined by conducting vulnerability assessments and monitoring attempts and successful breaches, and comparing the results of these activities with previous findings before the incentives.

LADWP appreciates the sustained efforts to improve the Nation's cybersecurity across all sectors as a matter of the national and economic security of the United States, and looks forward to continue contributing to this important effort.

Sincerely,

Randy S. Howard
Chief Compliance Officer - Power System
111 North Hope Street, Suite 921
Los Angeles, CA, 90012
Telephone Number: (213) 367-0381
Email: Randy.Howard@ladwp.com

MG:ms

SUBMITTED VIA EMAIL TO: cyberincentives@nist.doc.gov