From: Harry Silver <harry.silver.dhs@gmail.com>
Date: Monday, April 8, 2013 7:58 PM
To: cyberframework <cyberframework@nist.gov>
Cc: Adam Sedgewick <adam.sedgewick@nist.gov>
Subject: “Developing a Framework to Improve Critical Infrastructure Cybersecurity”

From: Harry Silver (harry.silver@hq.dhs.gov) ; Senior Advisor / Loaned Executive [703 325 2585 or 201 925 0040]

Three Critical Elements of the Framework--

1. S.M.A.R.T. Goals for implementation milestones and with accountability designated at the Role Level (Not department or organizational unit level in order to assure resiliency and minimize the difussion of accountability) such as Director-XYZ, NPPD.

2. Implementation must include a description of how voluntary adoption(or non-adoption) will be measured and reported. Frequency and distribution list or posting of exceptions-to-adoption reporting at a detailed level is required before final draft review is distributed.

3. The Framework needs to isolate ownership of accepted 'residual' risk at the primary ownership level and secondary level so that named(role) accountability drives prudent investment decisions at the O/O level as well as the Public Sector level.