

## Comments on MA Grid Modernization Working Group Report, 2 July 2013 version

The current version of the plan has one section to cover both Cyber Security and Privacy:

### 5.7. Cyber-Security and Privacy

*1. [Consensus Recommendation] Cyber-Security and privacy are key considerations and must be elements of any grid modernization plan filed by the Distribution Companies.*

*2. [Clean Energy Caucus/ Office of the Attorney General/Low Income Network/ MA DOER] The DPU should require the utilities to develop and seek approval of Cyber-Security plans, policies, and protocols as part of each grid modernization plan (as well as through any other regulatory procedures that the DPU may require). Utilities should have periodic reporting requirements to demonstrate compliance with protocols. (Note: Portion of the plans may require confidential treatment to ensure system security.)*

#### Comment:

The essence of this section is that cyber security and privacy are important and the utilities should report what they're doing to the DPU. However, the low level of detail seems substantially out of step with the high level of attention critical infrastructure cyber security is getting at the Federal level, as well as what's been developed and practiced in other states as well as other economic sectors.

#### Recommendation:

With cyber security being increasingly recognized as a material risk to the operations of electric utilities and regional grid infrastructure, the state of Massachusetts and its DPU can and should do much better.

Customized for the unique requirements of the Commonwealth, the cyber security and privacy elements of our grid modernization plan should leverage and reference guidance in this domain from a number of credible and established sources including DOE, NIST, NARUC and California PUC.

Particularly relevant and helpful documents include:

1. NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

[http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628\\_vol1.pdf](http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf)

2. NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

[http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628\\_vol2.pdf](http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf)

3. NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References

[http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628\\_vol3.pdf](http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf)

4. NARUC - Cybersecurity for State Regulators With Sample Questions for Regulators to Ask Utilities

<http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf>

5. DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

[http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20\(ES-C2M2\)%20-%20May%202012.pdf](http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf)

6. CPUC Policy Paper: Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission

<http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf>

7. State of California: Decision Adopting Rules To Protect The Privacy And Security Of The Electricity Usage Data Of The Customers Of Pacific Gas And Electric Company, Southern California Edison Company, And San Diego Gas & Electric Company

<http://www.sgclearinghouse.org/node/4534>

8. NIST Critical Infrastructure Security Framework (in development)

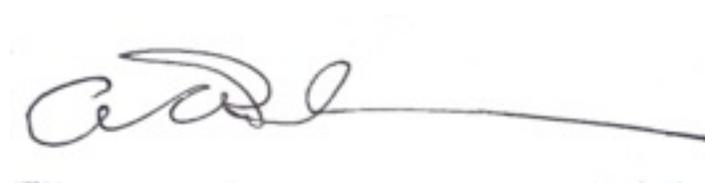
<http://www.nist.gov/itl/cyberframework.cfm>

While some or all of these will be familiar to the utility cyber security staff, the collected content of these resources might at first blush seem overwhelming to DPU personnel and advisors. However in each of these documents are a few key recommendations and best practices that the state could choose from and prioritize according to its business and risk management needs.

In particular I recommend DPU consider selective use of language in item #7 above, the State of California decision on privacy and the security of customer usage data.

I greatly appreciate the opportunity to share my remarks with you and will be happy to assist in the development of these concepts going forward.

Yours truly,

A handwritten signature in black ink, appearing to read 'A. Bochman', followed by a long horizontal line extending to the right.

Andrew A . Bochman  
Brookline, MA 02446