BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

Before the Public Utility Commission
Utility Commission

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's own Motion to Actively Guide Policy in California's Development of a Smart Grid System	Rulemaking 08-12-009 (Filed December 18, 2008)

Comments of the Electronic Privacy Information Center (EPIC) on Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart Grid and Customer Privacy

Lillie Coney, Associate Director, coney@epic.org
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW, Suite 200

Washington, DC 20009
202-483-1140

The Electronic Privacy Information Center (EPIC) would like to thank the California Public Utility Commission for its foresight and vision in setting in motion a policy making process to establish a baseline for the adoption and use of Smart Grid technologies in the state.

On March 9, 2010 EPIC filed comments with the Commission and offers the following recommendations for its further deliberation.

Our recommendations are as follows:

1. Adopt Smart Grid Fair Information Practices

Smart Grid Fair Information Practices Principle
Smart Grid service providers should limit collection of consumers' personal data; any such data collected should be obtained by lawful means and with the consent of the consumer, where appropriate.[1]
Data collected by Smart Grid service providers should be relevant to a specific purpose, and be accurate, complete, and up-to-date.
The purpose for collecting Smart Grid data should be settled at the outset.
The use of Smart Grid personal data ought to be limited to specified purposes, and data acquired for one purpose ought not be used for others.
Smart Grid data must be collected and stored in a way reasonably calculated to prevent its loss, theft, or modification.
There should be a general position of transparency with respect to the practices of handling Smart Grid data.
Smart Grid consumers should have the right to access, confirm, and demand correction of their personal data.
Those in charge of handling Smart Grid data should be responsible for complying with the principles of the privacy guidelines.

2. Adopt Privacy Impact Assessment Models for evaluation of privacy and Smart Grid applications and systems.[2]

[1] "Consent" is widely understood as "any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed." European Union Data Protection Directive, *reprinted in* The Privacy Law Sourcebook 450 (Marc Rotenberg ed., 2004).

[2] http://www.cio.gov/documents/pia_for_it_irs_model.pdf

3. Establish Independent Privacy Oversight – organizations and institutions responsible for providing Smart Grid services to consumers or oversight of companies engaged in providing services to consumers should establish independent privacy oversight within their organizations. Regulatory authorities should establish independent privacy oversight of companies engaged in Smart Grid service provision.

    - Privacy Officer should have experience in privacy law as well as policy
    - Privacy Office should be independent
    - Privacy oversight should be based on FIPs compliance
    - Privacy Office should have the resources to engaged in Privacy Impact Assessments on uses of personal information or new forms of personally identifiable information.

4. Abandon the Notice and Consent Model of privacy protection. Notice and choice has failed because of over reliance on it alone instead of all of the principles of fair information practices. Notice in exchanges where the customer has not alternatives, such as in the case of electricity service does not work.
5. Institute restrictions on data retention and use to only those necessary to provide a benefit or service related to Smart Grid.
6. Institute end-to-end security requirements for Smart Grid systems, eliminate the use of wireless technology, and establish strong security standards for all applications that will communicate with or receive communication from the Smart Grid network.
7. Verify techniques that are intended to anonymize data be sure that are effective and evaluate the potential for re-identification of individuals based on the anonymization process used.
8. Establish robust cryptographic standards to protect Smart Grid electricity usage data collection, retention, transfer, and use. Further evaluation and appropriate

measures should be taken to protect other forms of personal information retained by service providers.[3]

9. Adopt standards and certification requirements that match or exceed those for aviation or medical technology.
10. Define due process rights of individuals when law enforcement seeks Smart Grid information or access to network communications.
11. Prohibit participation in Fusion Centers or Federal or state information sharing environment programs.
12. Consider the relevance of residential and commercial electricity backup capacity in the event of Smart Grid or related system failures.

EPIC does support the goal that strong baseline standards are necessary to manage the adoption of Smart Grid technologies. The challenge for the commission will not be limited to guiding the work of tradition electricity energy suppliers, but the entry of non-traditional companies seeking to provide energy management services.

There are two kinds of harm that the Smart Grid might face: intentional and unintentional. Nature or the environment can cause harm, but it will never be based on an underlying intent. Utilities preparedness and response to hurricanes, tornadoes, ice storms, may in many ways resemble their response to man caused events that impact the reliability or availability of electricity.

However, the next greatest threat will be manmade intended or unintended consequences to the Smart Grid. New applications or devices added to a complex system of Smart Grid architecture may offer threats to reliability that might challenge service providers. Further, weaknesses in the underlying architecture; grid software and firmware development could also introduce vulnerabilities to information privacy and security. Further threats are posed by updates, or intentional exploitations of vulnerabilities or

[3] http://www.securecomputing.net.au/Feature/150901,hacking-the-smart-grid.aspx

weaknesses inherent in the complexity of Smart Grid systems. Additionally, the applications introduced by third party service providers may also pose risk to consumers.

For example: [4]

- Bypassing or overriding Smart Grid security protocols intended to protect personal or electricity usage data in transit or other critical functions by insiders. Errors in software design or intentional development of trapdoors during development or specifically for maintenance purposes that are exploited for unapproved or impermissible purposes.
- Inadequate identification, authentication, and authorization of users, tasks, and systems, which may result in system spoofing attacks when one component masquerades as another. In addition, incomplete or inconsistent authentication and validation problems can led to breaches of personal information or exploits against critical Smart Grid infrastructure.
- Other problems can include improper installation of technology, improper finalization of Smart Grid infrastructure and applications.
- Improper encapsulation where internal Smart Grid system or subsystem are made in accessible from the outside.
- Reliance upon clocks, internal sequential processes that must occur before other critical functions can occur that can led to system failures for securing of personal information or critical systems.
- Individuals who design and field Smart Grid energy management equipment independent of standards or oversight can pose risks to consumers. Customers of an energy usage management company in the United Kingdom's were adversely affected when the system failed. As they occurred, problems with the energy manage company's service were fixed on the fly and eventually the system became so complicated that they attempted to redesign it. The underlying problem that created an inherent vulnerability was how electricity managed by the energy usage

[4] Peter G. Neumann, Computer Related Risk, p. 105-108, 1995

> management company on its customers' behalf did not address backups should the system fail. Power supplied to the company's outstation fell below capacity and it tripped off heating systems. It was a very cold winter and after hours of waiting the power was restored. The failure resulted in the hospitalization of an elderly woman for hypothermia.[5]

Finally, the implications for protecting privacy of information stored on computers or exchanged on Smart Grid networks is whether data is or is not PII. This is information that can locate or identify a person, or can be used in conjunction with other information to uniquely identify an individual. Historically, PII would include name, social security number, address, phone number, or date of birth. In the Internet Age the list of PII has grown to include e-mail addresses, IP addresses, social networking pages, search engine requests, logons, or passwords.

Privacy violations can lead to threats to individuals in a number of instances.

For example,[6]

- A stalker killed Rebecca Schaeffer, a television actress after he used publically available California Division of Motor Vehicle (DMV) records to locate her home address.
- A former Arizona law-enforcement officer collected information from three different sources to track down his estranged girl friend and murdered her.
- An Anaheim Police Department employee used access to DMV records to identify the home of a person targeted by anti-abortion group, which led to the Tustin, California home being picketed in February 1993.

Possibility of Significant Privacy Harms Posed by Wireless Smart Grid Applications

[5] http://catless.ncl.ac.uk/Risks/5.67.html#subj7.1
[6] il, footnote 10

Wireless Smart Grid technology used to transmit user electricity consumption data must protect privacy. Wireless sensors and networks are susceptible to security breaches unless properly secured, and breaches of wireless technology could expose users' personal data.

"War Driving" thieves search for open unprotected wireless communication devices for the purpose of using it for communication purposes, or to steal data being transmitted over the device.

For example:

> "War driving" hackers will search for unprotected wireless devices at shopping centers and strip malls. If the security of the device used by shopping centers or malls has weak wireless security, hackers will exploit it for the data they can obtain remotely. They can be stationed in a car parking lot outside of the structure where the wireless device is located.[7] The largest known security beach due to "War Driving" involved the theft of 45 million credit cards from the TJ Max and Marshalls's chain of stores when hackers found vulnerability in the wireless technology used by the retailers.[8]

The degree to which Smart Grid systems and related applications would recalculate the formulation of what is knowable about the intimate details of home life by adding to the list of PII, or expanding on the collection, retention, use, and sharing of PII pose significant risk to consumers of electricity.

[7] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4470120.ece

[8] http://www.informationweek.com/news/mobility/showArticle.jhtml?articleID=199500385

The conservative view of data security is to stop any possible bad thing by keeping knowledge bottled up. The converse view is to know everything knowable about everyone who might have some input or influence over a protected system. The first approach faces challenges in the "Digital Information Age" because anything that is knowable is learnable and therefore sharable. The Second approach poses serious problems for a free and democratic society.

The course that the commission will chart will be ground breaking. The rights of consumers in the digital information age require strong leadership on the part of regulators and policy makers.

Conclusion

Privacy protection is essential to the successful implementation of the Smart Grid and failure to develop robust and implement privacy policy will hinder adoption of applications and services. EPIC is willing and able to contribute the further development of Smart Grid Privacy policy and look forward to the opportunity to collaborate with others toward this end. We thank the California Public Utility Commission for its dedication to protect the rights of consumers and the future implications for extending those rights to U.S. consumers.

Sincerely,

/s/Lillie Coney

Lillie Coney, Associate Director
EPIC
April 7, 2010

CERTIFICATE OF SERVICE

I Lillie Coney, am over the age of 18 years and employed by the Electronic Privacy Information Center based in Washington, DC. My business address is 1718 Connecticut Avenue, NW, Suite 200, Washington, DC 20009.

On April 14, 2010, I served the within Document Reply Comments of the Electronic Privacy Information Center in R08-12-009, with service on the service list for R 08-12-009 in compliance with the Commission's Rules of Practice and Procedure and separate and additional delivery of hard copies by U.S. Mail to Assigned Commissioner Ryan and Assigned ALJ Sullivan, at San Francisco, California.

Executed on April 14, 2010, at Washington, DC.

/s/ Lillie Coney
Lillie Coney
EPIC

R-08-12-009 SERVICE LIST

carlgustin@groundedpower.com
jeffrcam@cisco.com
dbrenner@qualcomm.com
coney@epic.org
cbrooks@tendrilinc.com
npedersen@hanmor.com
slins@ci.glendale.ca.us
douglass@energyattorney.com
xbaldwin@ci.burbank.ca.us
kris.vyas@sce.com
ATrial@semprautilities.com
lburdick@higgslaw.com
liddell@energyattorney.com
mshames@ucan.org
ctoca@utility-savings.com
bobsmithttl@gmail.com
mtierney-lloyd@enernoc.com
ed@megawattsf.com
mterrell@google.com
mdjoseph@adamsbroadwell.com
elaine.duncan@verizon.com
pickering@energyhub.net
margarita.gutierrez@sfgov.org
lms@cpuc.ca.gov
fsmith@sfwater.org
srovetti@sfwater.org
tburke@sfwater.org
lettenson@nrdc.org
marcel@turn.org
mkurtovich@chevron.com
cjw5@pge.com
keith.krom@att.com
nes@a-klaw.com
pcasciato@sbcglobal.net
steven@sfpower.org
tien@eff.org
mgo@goodinmacbride.com
mday@goodinmacbride.com
ssmyers@worldnet.att.net
lex@consumercal.org
farrokh.albuyeh@oati.net
Service@spurr.org
wbooth@booth-law.com
lencanty@blackeconomiccouncil.org
jwiedman@keyesandfox.com
kfox@keyesandfox.com
enriqueg@greenlining.org

gmorris@emf.net
robertginaizda@gmail.com
aaron.burstein@gmail.com
dkm@ischool.berkeley.edu
longhao@berkeley.edu
jlynch@law.berkeley.edu
kerry.hattevik@nrgenergy.com
rquattrini@energyconnectinc.com
seboyd@tid.org
martinhomec@gmail.com
dzlotlow@caiso.com
dennis@ddecuir.com
scott.tomashefsky@ncpa.com
jhawley@technet.org
lnavarro@edf.org
Lesla@calcable.org
cbk@eslawfirm.com
gstaples@mendotagroup.net
jlin@strategen.com
MNelson@MccarthyLaw.com
EGrizard@deweysquare.com
r.raushenbush@comcast.net
tam.hunt@gmail.com
john.quealy@canaccordadams.com
mark.sigal@canaccordadams.com
barbalex@ctel.net
crjohnson@lge.com
julien.dumoulin-smith@ubs.com
david.rubin@troutmansanders.com
jennsanf@cisco.com
marybrow@cisco.com
jmccarthy@ctia.org
jay.birnbaum@currentgroup.com
bboyd@aclaratech.com
bob.rowe@northwestern.com
monica.merino@comed.com
sthiel@us.ibm.com
ed.may@itron.com
rgifford@wbklaw.com
leilani.johnson@ladwp.com
jorgecorralejo@sbcglobal.net
dschneider@lumesource.com
david@nemtzow.com
cjuennen@ci.glendale.us
mark.s.martinez@sce.com
case.admin@sce.com
michael.backstrom@sce.com

nquan@gswater.com
Jcox@fce.com
esther.northrup@cox.com
kfoley@sempra.com
kmkiener@cox.net
djsulliv@qualcomm.com
rwinthrop@pilotpowergroup.com
CentralFiles@semprautilities.com
jon.fortune@energycenter.org
sephra.ninow@energycenter.org
tcahill@semprautilities.com
cmanson@semprautilities.com
jerry@enernex.com
traceydrabant@bves.com
peter.pearson@bves.com
dkolk@compenergy.com
ek@a-klaw.com
rboland@e-radioinc.com
sue.mara@rtoadvisors.com
juan.otero@trilliantinc.com
mozhi.habibi@ventyx.com
faramarz@ieee.org
mandywallace@gmail.com
norman.furuta@navy.mil
kgrenfell@nrdc.org
mcarboy@signalhill.com
nsuetake@turn.org
bfinkelstein@turn.org
andrew_meiman@newcomb.cc
ayl5@pge.com
regrelcpuccases@pge.com
DNG6@pge.com
fsc2@pge.com
filings@a-klaw.com
Kcj5@pge.com
mpa@a-klaw.com
rcounihan@enernoc.com
stephen.j.callahan@us.ibm.com
tmfry@nexant.com
info@tobiaslo.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
cassandra.sweet@dowjones.com
jscancarelli@crowell.com
jas@cpdb.com
joshdavidson@dwt.com
nml@cpdb.com
SDHilton@stoel.com
katienelson@dwt.com
suzannetoller@dwt.com
Diane.Fellman@nrgenergy.com
cem@newsdata.com
lisa_weinzimer@platts.com
prp1@pge.com
achuang@epri.com
caryn.lai@bingham.com
epetrill@epri.com
ali.ipakchi@oati.com
chris@emeter.com
sharon@emeter.com
ralf1241a@cs.com
mike.ahmadi@Granitekey.com
sean.beatty@mirant.com
john_gutierrez@cable.comcast.com
lewis3000us@gmail.com
Valerie.Richardson@us.kema.com
nellie.tong@us.kema.com
Douglas.Garrett@cox.com
rstuart@brightsourceenergy.com
mrw@mrwassoc.com
cpucdockets@keyesandfox.com
dmarcus2@sbcglobal.net
rschmidt@bartlewells.com
RobertGnaizda@gmail.com
jurban@law.berkeley.edu
kco@kingstoncole.com
philm@scdenergy.com
j_peterson@ourhomespaces.com
joe.weiss@realtimeacs.com
michaelboyd@sbcglobal.net
bmcc@mccarthylaw.com
sberlin@mccarthylaw.com
mary.tucker@sanjoseca.gov
tomk@mid.org
joyw@mid.org
brbarkovich@earthlink.net
gayatri@jbsenergy.com
dgrandy@caonsitegen.com
demorse@omsoft.com
martinhomec@gmail.com
e-recipient@caiso.com
hsanders@caiso.com
jgoodin@caiso.com
wamer@kirkwood.com
tpomales@arb.ca.gov
brian.theaker@dynegy.com
danielle@ceert.org
wmp@cpuc.ca.gov

jmcfarland@treasurer.ca.gov
shears@ceert.org
kellie.smith@sen.ca.gov
lkelly@energy.state.ca.us
mgarcia@arb.ca.gov
ro@calcable.org
steven@lipmanconsulting.com
lmh@eslawfirm.com
abb@eslawfirm.com
bsb@eslawfirm.com
glw@eslawfirm.com
jparks@smud.org
ljimene@smud.org
ttutt@smud.org
vzavatt@smud.org
vwood@smud.org
dan.mooy@ventyx.com
kmills@cfbf.com
rogerl47@aol.com
jellis@resero.com
michael.jung@silverspringnet.com
wmc@a-klaw.com
bschuman@pacific-crest.com
sharon.noell@pgn.com
californiadockets@pacificorp.com
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
am1@cpuc.ca.gov
crv@cpuc.ca.gov
df1@cpuc.ca.gov
dbp@cpuc.ca.gov
trh@cpuc.ca.gov
fxg@cpuc.ca.gov
gtd@cpuc.ca.gov
jw2@cpuc.ca.gov
jdr@cpuc.ca.gov
jmh@cpuc.ca.gov
kar@cpuc.ca.gov
kd1@cpuc.ca.gov
lau@cpuc.ca.gov
zaf@cpuc.ca.gov
mjd@cpuc.ca.gov
mc3@cpuc.ca.gov
wtr@cpuc.ca.gov
rhh@cpuc.ca.gov
srt@cpuc.ca.gov
scr@cpuc.ca.gov
tjs@cpuc.ca.gov
vjb@cpuc.ca.gov
BLee@energy.state.ca.us
ab2@cpuc.ca.gov

Communication Sent By FIRST CLASS U.S. Mail

Harold Galicer
Seakay, Inc
PO Box 78192
San Francisco, CA94107

Kevin Anderson
UBS Investment Research
1285 Avenue of the Americas
New York, NY 10019

Jim Sueuga
Valley Electric Association
P.O. Box 237
Pahrump, NV 89041

Phil Jackson
System Engineer
Valley Electric Association
800 E. HWY 372
PO BOX 237
Pahrump, NV 89041

Megan Kuize
Dewey & Lebouf
1950 University Circle, Suite 500
East Palo Alto, CA 94303

David Kates
David Mark & Company
3510 UNOCAL PLACE, SUITE 200
Santa Rosa, CA 95403

Jessica Nelson
Energy Services Manager
Plumas Sierra Rural Electric Coop
73233 State Route 70
Portola, CA 96122-7069