



BEFORE THE PUBLIC UTILITIES COMMISSION OF THE
STATE OF CALIFORNIA

FILED
06-10-10
04:59 PM

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 CYBERSECURITY AND PRIVACY LAW AND POLICY
RESEARCHERS ON PROPOSED DECISION ADOPTING REQUIREMENTS FOR
SMART GRID DEPLOYMENT PLANS PURSUANT TO SENATE BILL 17 (PADILLA),
CHAPTER 327, STATUTES OF 2009**

Aaron J. Burstein
Deirdre K. Mulligan
University of California, Berkeley*
School of Information
South Hall
Berkeley, CA 94720

* Institutional affiliation is provided for identification purposes only. The views expressed in this comment do not purport to represent those of the University of California.

Dated: June 10, 2010

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

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 CYBERSECURITY AND PRIVACY LAW AND POLICY
RESEARCHERS ON PROPOSED DECISION ADOPTING REQUIREMENTS FOR
SMART GRID DEPLOYMENT PLANS PURSUANT TO SENATE BILL 17 (PADILLA),
CHAPTER 327, STATUTES OF 2009**

Pursuant to Rule 14.3 of the Commission's Rules of Practice and Procedure, we submit these comments on the Proposed Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, filed May 21, 2010 ("Proposed Decision").

I. INTRODUCTION

We appreciate the opportunity to comment on the Proposed Decision. This brief comment focuses on the Proposed Decision's requirements for the cyber security section of Smart Grid deployment plans.

The importance of cyber security in this proceeding is beyond debate.¹ As the Proposed Decision notes, “[a]ll parties who discussed security agree with the Commission that security of California’s electric grid, including cyber security, is critical.”² The Proposed Decision gives cyber security due consideration, and its cyber security requirements take several steps in the direction of maintaining the security of the electric grid.

The Proposed Decision, however, fails to fully address cyber security issues that several parties raised in their comments about the importance of building cyber security mechanisms into the Smart Grid and subjecting cyber security strategies and mechanisms to independent scrutiny. These comments suggest two modifications that would bring the Proposed Decision into line with the record.

II. DISCUSSION

A. It is Reasonable to Defer Adoption of Requirements in Light of the Unsettled State of National Smart Grid Cyber Security Standards.

Noting the general consensus among parties that “the developing NIST [National Institute of Standards and Technology] framework will address many of the security issues that are arising,”³ but that the framework is not yet final, the Proposed Decision states that it would be “premature to adopt specific Smart Grid security standards at this time.”⁴ Instead, the Proposed Decision requires deployment plans to “use” the NIST cyber security framework, in

¹ This is not to ignore the importance of privacy. As the Proposed Decision notes, however, the Commission will take up privacy rules in a later phase of the proceeding. Proposed Decision at

² Proposed Decision at 47. *See also id.* at 48-55 (quoting supporting comments from utilities, device and networking equipment manufacturers, and public interest groups).

³ Proposed Decision at 56.

⁴ Proposed Decision at 58. The framework referred to in the main text is *Second DRAFT NIST IR 7628 Smart Grid Cyber Security Strategy and Requirements*, Feb. 2010, at <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628>.

addition to cyber security guidelines developed by the Department of Homeland Security.⁵ This is a reasonable and constructive use of existing guidance until the Commission adopts cyber security requirements.

The Proposed Decision, however, leaves two gaps in the deployment plan requirements.

B. The Proposed Decision Should Require More Detailed Information About Cyber Security Assessments.

First, the operative language in the Conclusions of Law is vague. Requiring deployment plans to “address” or “use” cyber security guidance documents⁶ provides little assurance that the plans will provide information sufficient to meet the underlying goal of ensuring that cyber security is “considered explicitly at the planning stage.”⁷ To achieve this goal, deployment plans should show enough work to inform the Commission, and members of the public, *how* the utilities have (or have not) taken the relevant requirements into account.

To take one example, Requirement 2.8.5.1 in the *Catalog of Control Systems Security* states: “The control system protects against or limits the effects of denial-of-service attacks based on an organization’s defined list of types of denial-of-service attacks.”⁸ It is unclear what kind of response would “address” this requirement. Ideally, a response to this requirement would refer to the relevant components of the system’s architecture; describe the denial-of-service threats that the utility has considered in terms of this architecture; state what technical

⁵ Proposed Decision at 122 (citing three documents that set guidelines for control system security).

⁶ Proposed Decision at 117, 122.

⁷ Proposed Decision at 3-4 (explaining how the cyber security requirements for deployment plans effect the legislative goal, as expressed in Senate Bill 17, Cal. Pub. Utils. Code § 8360, of “cost-effective full cyber security”). See also Proposed Decision at 29-30 (elaborating SB 17’s cyber security requirement in terms of attack resistance, resilience, response, and mitigation).

⁸ U.S. Dept. of Homeland Security, *Catalog of Control Systems Security: Recommendations for Standards Developers* 38, Mar. 2010, available at http://www.us-cert.gov/control_systems/pdf/Catalog%20of%20Recommendations%20March%202010.pdf; Proposed Decision at 58 n.151 (citing this document).

and procedural mechanisms it has in place to protect against or limit such attacks; and whether those mechanisms have been tested. In other words, the deployment plan should contain a threat model, which specifies an attacker's goals and explains in terms of a system's architecture and data flow how those goals might be achieved,⁹ and information about the status of security testing.

This level of detail is necessary to allow the Commission to ensure that cyber security is and remains a Smart Grid design requirement. Numerous parties have expressed support for this “security by design” idea. For example, San Diego Gas & Electric (SDG&E) “advocates a proactive and preventative security approach which programmatically addresses architectural, design, engineering, comprehensive testing, and operational monitoring and maintenance stages of the cyber security lifecycle.”¹⁰ Verizon states that “[i]t is important that security be designed into the initial smart grid plan and that security remains an integral part of the overall design and deployment of smart grid technology and applications.”¹¹ Finally, Cisco notes that “the CPUC and [investor owned utilities] have an opportunity to work together to ‘bake-in’ security from the outset, as new technologies are brought online.”¹²

Recommendation. A simple way to fix the deficiency in the Proposed Decision is to make the ordering language more explicit. In addition to requiring utilities to “use” the cited guidelines, the Commission should direct them to specify (1) what testing they have done (or

⁹ See generally SANS Institute, *Threat Modeling: A Process to Ensure Application Security*, Jan. 5, 2005, at http://www.sans.org/reading_room/whitepapers/securecode/threat-modeling-process-ensure-application-security_1646.

¹⁰ SDG&E Opening Comments at 17.

¹¹ Verizon Opening Comments at 8. See also *id.* (“The Commission is in a unique position to integrate security measures into the *initial* design, development and provisioning of a smart grid network in California.”) (emphasis in original).

¹² Cisco Opening Comments at 18.

rely on, if the testing was performed by another entity) to gauge their systems against the guidelines; (2) what results they have obtained from this testing; and (3) what criteria they use to determine whether specific requirements are inapplicable. This change would not be tantamount to adopting these guidelines as mandatory standards; the Proposed Decision does not set criteria for determining which requirements are applicable or specify a course of action (e.g., cessation of deployment) if a system fails to meet a requirement. The Commission will need to make those kinds of decisions later, when it adopts cyber security standards and a structure for conformance testing and certification.¹³ The changes to Proposed Decision that are suggested here will provide the Commission with better information when it makes those decisions.

C. The Proposed Decision Should Balance the Need for Public Disclosure of Cyber Security-Related Information with the Need to Protect Sensitive Information.

Second, the Commission should qualify the Proposed Decision’s invitation to utilities to file materials concerning cyber security “under seal.”¹⁴ On one hand, it is likely that some of this information will be sensitive, either because it contains trade secrets or other confidential information, or because it describes vulnerabilities that remain open. On the other hand, the Commission and several parties have emphasized that public discussion of cyber security issues is essential to building trust in the Smart Grid.¹⁵

¹³ After adopting those standards, of course, the Commission will need to determine whether systems conform with them. The NIST-led conformance activity might provide this determination. But national conformance testing and certification is still under development. The deployment plan requirement set forth above would serve California well in the meantime.

¹⁴ Proposed Decision at 59.

¹⁵ See Proposed Decision at 56 (“The Commission and the public have a right to be assured that the electric grid will remain secure with the deployment of Smart Grid technologies.”); *id.* (“The Smart Grid deployment plans can provide the Commission and the public with insight into the security of the Smart Grid.”). *Accord* CDT/EFF Opening Comments at 23 (explaining how

Recommendations. One way to reduce this tension is to provide more detailed criteria for sealing documents. The Proposed Decision, for example, could announce a Commission policy of making cyber security information in deployment plans public “to the fullest possible extent,”¹⁶ allowing utilities to file documents under seal if they state an appropriate reason. This need not be a binary decision; redacting sensitive information within a document can help strike the right balance.

A complementary approach would be to convene an independent advisory board to review full, unredacted deployment plans. This would allow full public review of redacted deployment plans while providing independent review of the full plans. Members of this board could provide the Commission with additional expertise (e.g., in the area of control system security) to assess the cyber security elements of deployment plans. In addition, the advisory board could be empowered to report on its findings, thereby educating the Commission and members of the public on Smart Grid cyber security.

There is precedent for this kind of arrangement in California. For example, California Secretaries of State have assembled numerous task forces and advisory boards to assess voting system security, among other technical issues: the Internet Voting Task Force;¹⁷ the Voting System Technology Assessment Advisory Board (VSTAAB);¹⁸ and the Top-to-Bottom

security breach notification requirements can “help the public and the Commission to evaluate regulable entities’ security efforts”); Researchers Opening Comment at 18-19.

¹⁶ Researchers Opening Comments at 17.

¹⁷ California Sec. of State, California Internet Voting Task Force, Jan. 18, 2000, at <http://www.sos.ca.gov/elections/ivote/>.

¹⁸ For a VSTAAB report on vulnerabilities in a specific voting system, see David Wagner, David Jefferson, Matt Bishop, Chris Karlof, and Naveen Sastry, *Security Analysis of the Diebold AccuBasic Interpreter*, Feb. 14, 2006, http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf.

Review.¹⁹ These expert reviews provided independent, scientifically sound assessments of voting system security. We emphasize that these reviews found many vulnerabilities *after* the systems had undergone national-level and state testing and certification. Another model is the California Privacy and Security Advisory Board, which advises the California Office of Health Information Integrity on privacy and security issues concerning electronically exchanged health information.²⁰ These examples demonstrate that advisory boards and task forces can be helpful on matters ranging from broad strategic considerations to evaluations of specific technological artifacts.

An advisory board or task force structure could be extremely useful in the Smart Grid cyber security context. Assembling a task force or advisory board now would have the advantage of providing a close examination of Smart Grid cyber security at an early stage of system deployment. This institutional arrangement can allow utilities, the Commission, and other stakeholders to share knowledge, address vulnerabilities early in the development of the grid, and likely reduce costs in the long run.²¹

¹⁹ California Sec. of State, Top-to-Bottom Review, <http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm> (last visited June 9, 2010).

²⁰ See California Office of Health Information Integrity, California Privacy and Security Advisory Board Overview, <http://www.ohi.ca.gov/calohi/PSAB/AdvisoryBoard.aspx#Overview> (last visited June 9, 2010).

²¹ See Telecommunications Industry Association (TIA) Reply Comments at 5-6 (recommending that the Commission “seek the opinion of a qualified and neutral third party when evaluating and rendering Smart Grid decisions that involve ICT”). TIA further notes that “Smart Grid decisions based on inadequate information may result in system vulnerabilities that negatively impact the reliability of energy services, the privacy of ratepayers, and the ability of the Smart Grid to deliver on its full potential. It may further result in undesirable post-deployment costs to remediate security shortcomings that could have been avoided through an independent information security assessment during the planning stage.” *Id.* at 6. AT&T, Cisco, and Verizon also emphasize in their comments the importance of sharing expertise and seeking peer review in the cyber security domain. See AT&T California Opening Comments at 7, 16-17 (suggesting that expertise from commercial communications network operators is relevant to Smart Grid cyber security); Cisco Opening Comments at 16 (stating that “substantial peer-review and

III. CONCLUSION

For the reasons stated above, we respectfully request that the Proposed Decision's Findings of Fact, Conclusions of Law, and Ordering Paragraphs be modified in accordance with the language set forth in the Appendix.

Respectfully submitted this June 10, 2010, at Baltimore, Maryland,

/s/ Aaron J. Burstein
AARON J. BURSTEIN

/s/ Deirdre K. Mulligan
DEIRDRE K. MULLIGAN

University of California, Berkeley*
School of Information
South Hall
Berkeley, CA
Telephone: (510) 410-6964
Email: aaron.burstein@gmail.com

significant investment by security experts and organizations provide a firm foundation for standards-based security technology"); Verizon Opening Comments at 8 (citing examples of industry-wide security practices in healthcare and payment cards).

* Institutional affiliation is provided for identification purposes only. The views expressed in this comment do not purport to represent those of the University of California.

SUBJECT INDEX

Creating advisory board or task force for cyber security issues	pp. 6-7
Requiring threat models in deployment plans	pp. 3-5
Setting criteria for sealing information in deployment plans	pp. 5-6

**APPENDIX: PROPOSED FINDINGS OF FACT
AND CONCLUSIONS OF LAW**

PROPOSED FINDINGS OF FACT

ADD Finding of Fact: Designing cyber security into the Smart Grid will reduce the vulnerability of the electric grid and reduce the likelihood of later needing to modify Smart Grid components to address vulnerabilities.

ADD Finding of Fact: Threat modeling—identifying an attacker’s goals and specifying how those goals might be accomplished in a given system—provides a valuable and systematic way of identifying vulnerabilities in systems such as the electric grid.

ADD Finding of Fact: Subjecting Smart Grid cyber security assessments to the broadest possible review will improve their quality and allow utilities and the Commission to take advantage of industry, academic, and public interest expertise.

PROPOSED CONCLUSIONS OF LAW

MODIFY Conclusion of Law 18: It is reasonable to require that the Grid Security and Cyber Security Strategy section of the Smart Grid deployment plans ~~address~~ specify, for each applicable requirement in the guidance documents that NIST and DHS are developing, (1) what testing or analysis a utility has done (or relies on, if the testing or analysis was performed by another entity) to gauge their systems against the requirement; (2) what results were obtained from this testing or analysis; and (3) what criteria were used to determine whether specific requirements are inapplicable.

ADD Conclusion of Law: It is reasonable to require utilities to request that specific portions of deployment plans be filed under seal, and to state the reason(s) for each request, subject to the Commission's approval or redaction.

PROPOSED ORDERING PARAGRAPHS

MODIFY Ordering Paragraph 1: Pacific Gas and Electric Company, Southern California

Edison Company and San Diego Gas & Electric Company each shall file an application no later than July 1, 2011 submitting its Smart Grid deployment plan, consistent with Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009, and the requirements in this decision. If a utility requests to submit any portion of its deployment plan under seal, it shall designate those portions with specificity and state the reason(s) for its request to file under seal. Each utility shall serve its application on the service lists for Rulemaking 08-12-009 and any open Long Term Procurement Plan proceedings. If the utility has a pending general rate case proceeding, it shall also serve its application on that proceeding's service list.

MODIFY Ordering Paragraph 8: Pacific Gas and Electric Company, Southern California

Edison Company and San Diego Gas & Electric Company each shall use, in the section on Grid Security and Cyber Security Strategy in its Smart Grid deployment plan, the guidance documents that the National Institute of Standards and Technology and the United States Department of Homeland Security have developed or are developing to promote cyber security. Specifically, cyber security sections must use the latest versions of the following three documents to guide their preparations:

- a. Security Profile for Advanced Metering Infrastructure, v 1.0, Advanced Security Acceleration Project – Smart Grid, December 10, 2009;

- b. Catalog of Control Systems Security: Recommendations for Standards Developers, United States Department of Homeland Security, National Cyber Security Division, September; and
- c. United States Department of Homeland Security Cyber Security Procurement Language for Control Systems.

For each applicable requirement in documents listed above, cyber security sections shall state (1) what testing or analysis has been performed (or is relied on, if the testing was performed by another entity) to gauge a system against the requirements; (2) what results were obtained from this testing or analysis; and (3) what criteria were used to determine whether specific requirements are inapplicable.

CERTIFICATE OF SERVICE

I certify that, pursuant to the Commission's Rules of Practice and Procedure, I have served a true copy of **COMMENTS OF PRIVACY AND CYBERSECURITY LAW AND POLICY RESEARCHERS ON PROPOSED DECISION ADOPTING REQUIREMENTS FOR SMART GRID DEPLOYMENT PLANS PURSUANT TO SENATE BILL 17 (PADILLA), CHAPTER 327, STATUTES OF 2009** on all parties identified in the attached service lists. Service was effected through the means indicated below:

Transmitting copies to all parties who have provided an email address; sending copies via first-class mail to all parties who cannot be served electronically; and sending copies via e-mail and first class mail to Administrative Law Judge Timothy Sullivan and Andrew Campbell, advisor to Commissioner Nancy Ryan.

Executed this June 10, 2010, at Baltimore, Maryland.

/s/ Aaron J. Burstein

AARON J. BURSTEIN
Research Fellow
University of California, Berkeley
School of Information
South Hall
Berkeley, CA 94720

SERVICE LIST

Last changed June 8, 2010

Andrew Campbell
Advisor to Commissioner Nancy Ryan
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA 94102-3214

Administrative Law Judge Timothy Sullivan
California Public Utilities Commission
505 Van Ness Avenue
San Francisco, CA 94102-3214

aaron.burstein@gmail.com
ab2@cpuc.ca.gov
abb@eslawfirm.com
achuang@epri.com
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
ali.ipakchi@oati.com
aml@cpuc.ca.gov
andrew_meiman@newcomb.cc
ATrial@SempraUtilities.com
ayl5@pge.com
barbalex@ctel.net
bboyd@aclaratech.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
bfinkelstein@turn.org
BKallo@rwbaird.com
BLee@energy.state.ca.us
bmcc@mccarthyllaw.com
bob.rowe@northwestern.com
bobsmithtl@gmail.com
brbarkovich@earthlink.net
brian.theaker@dynegy.com
bsb@eslawfirm.com
bschuman@pacific-crest.com
californiadockets@pacificorp.com
carlgustin@groundedpower.com
caryn.lai@bingham.com
case.admin@sce.com
cassandra.sweet@dowjones.com
cbk@eslawfirm.com
cbrooks@tendriline.com
cem@newsdata.com
CentralFiles@SempraUtilities.com
chris@emeter.com
cjuennen@ci.glendale.us
cjw5@pge.com
CManson@SempraUtilities.com
coney@epic.org

dbp@cpuc.ca.gov
dbrenner@qualcomm.com
demorse@omsoft.com
dennis@ddecuir.com
df1@cpuc.ca.gov
dgrandy@caonsitegen.com
Diane.Fellman@nrgenergy.com
djsulliv@qualcomm.com
dkm@ischool.berkeley.edu
dkolk@compenergy.com
dmarcus2@sbcglobal.net
DNG6@pge.com
DNiehaus@SempraUtilities.com
Douglas.Garrett@cox.com
douglass@energyattorney.com
dschneider@lumesource.com
dzlotlow@caiso.com
ed.may@itron.com
ed@megawattsf.com
EGrizard@deweysquare.com
ek@a-klaw.com
elaine.duncan@verizon.com
enriqueg@greenlining.org
epetrill@epri.com
e-recipient@caiso.com
esther.northrup@cox.com
faramarz@ieee.org
farrokh.albuyeh@oati.net
filings@a-klaw.com
fsc2@pge.com
fsmith@sflower.org
fxg@cpuc.ca.gov
gayatri@jbsenergy.com
GHealy@SempraUtilities.com
glw@eslawfirm.com
gmorris@emf.net
gstaples@mendotagroup.net
gtd@cpuc.ca.gov
hsanders@caiso.com

cpucdockets@keyesandfox.com
crjohnson@lge.com
crv@cpuc.ca.gov
ctoca@utility-savings.com
dan.mooy@ventyx.com
danielle@ceert.org
dave@ppallc.com
david.rubin@troutmansanders.com
david@nemtzwow.com
jerry@enernex.com
jgoodin@caiso.com
jhawley@technet.org
jlin@strategen.com
jlynch@law.berkeley.edu
jmccarthy@ctia.org
jmcfarland@treasurer.ca.gov
jmh@cpuc.ca.gov
joe.weiss@realttimeacs.com
john.quealy@canaccordadams.com
john_gutierrez@cable.comcast.com
jon.fortune@energycenter.org
jorgecorralej@sbcbglobal.net
joshdavidson@dwt.com
joyw@mid.org
jparks@smud.org
jscancarelli@crowell.com
jskromer@qmail.com
juan.otero@trilliantinc.com
judith@tothept.com
julien.dumoulin-smith@ubs.com
jurban@law.berkeley.edu
jw2@cpuc.ca.gov
jwiedman@keyesandfox.com
kar@cpuc.ca.gov
Kcj5@pge.com
kco@kingstoncole.com
kd1@cpuc.ca.gov
keith.krom@att.com
kellie.smith@sen.ca.gov
kerry.hattevik@nrgenergy.com
KFoley@SempraUtilities.com
kfox@keyesandfox.com
kgrenfell@nrdc.org
kmills@cxfb.com
kmiener@cox.net
kris.vyas@sce.com
lau@cpuc.ca.gov
lburdick@higgslaw.com
leilani.johnson@ladwp.com

info@tobiaslo.com
j_peterson@ourhomespaces.com
jandersen@tiaonline.org
jas@cpdb.com
jay.birnbaum@currentgroup.com
Jcox@fce.com
jdr@cpuc.ca.gov
jeffrcam@cisco.com
jellis@resero.com
lmh@eslawfirm.com
lms@cpuc.ca.gov
lnavarro@edf.org
longhao@berkeley.edu
mandywallace@gmail.com
marcel@turn.org
margarita.gutierrez@sfgov.org
mariacarb@dw.com
mark.s.martinez@sce.com
mark.sigal@canaccordadams.com
martinhom@ec@gmail.com
martinhom@ec@gmail.com
mary.tucker@sanjoseca.gov
marybrow@cisco.com
mc3@cpuc.ca.gov
mcarboy@signalhill.com
mcoop@homegridforum.org
mday@goodinmacbride.com
mdjoseph@adamsbroadwell.com
mgarcia@arb.ca.gov
mgo@goodinmacbride.com
michael.backstrom@sce.com
michael.jung@silverspringnet.com
michael.sachse@opower.com
michael_w@copper-gate.com
michaelboyd@sbcbglobal.net
mike.ahmadi@Granitekey.com
mjd@cpuc.ca.gov
mkurtovich@chevron.com
MNelson@MccarthyLaw.com
monica.merino@comed.com
mozhi.habibi@ventyx.com
mpa@a-klaw.com
mrw@mrwassoc.com
mshames@ucan.org
mterrell@google.com
mtierney-lloyd@enernoc.com
nellie.tong@us.kema.com
nes@a-klaw.com
nml@cpdb.com

lencanty@blackeconomiccouncil.org
Lesla@calcable.org
lettenson@nrdc.org
lewis3000us@gmail.com
lex@consumercal.org
liddell@energyattorney.com
lisa_weinzimer@platts.com
ljimene@smud.org
lkelly@energy.state.ca.us
puja@opower.com
r.raushenbush@comcast.net
ralf1241a@cs.com
rboland@e-radioinc.com
rcounihan@enernoc.com
regrelpuccases@pge.com
rgifford@wbklaw.com
rhh@cpuc.ca.gov
ro@calcable.org
robertginaizda@gmail.com
RobertGnaizda@gmail.com
rogerl47@aol.com
rquattrini@energyconnectinc.com
rschmidt@bartlewells.com
rstuart@brightsourceenergy.com
rwinthrop@pilotpowergroup.com
salleyoo@dwt.com
sberlin@mccarthy.com
scott.tomashefsky@ncpa.com
scr@cpuc.ca.gov
SDHilton@stoel.com
sean.beatty@mirant.com
seboyd@tid.org
sephra.ninow@energycenter.org
Service@spurr.org
sharon.noell@pgn.com
sharon@emeter.com
shears@ceert.org
slins@ci.glendale.ca.us
srovetti@sflower.org
ssmyers@worldnet.att.net
stephen.j.callahan@us.ibm.com
steven@lipmanconsulting.com
steven@sflower.org
sthiel@us.ibm.com
sue.mara@rtoadvisors.com
suzannetoller@dwt.com
tam.hunt@gmail.com
tburke@sflower.org
TCahill@SempraUtilities.com

norman.furuta@navy.mil
npedersen@hanmor.com
nquan@gswater.com
nsuetake@turn.org
pcasciato@sbcglobal.net
peter.pearson@bves.com
philm@scdenergy.com
pickering@energyhub.net
prp1@pge.com
Valerie.Richardson@us.kema.com
vjb@cpuc.ca.gov
vladimir.oksman@lantiq.com
vwood@smud.org
vzavatt@smud.org
wamer@kirkwood.com
wbooth@booth-law.com
wmc@a-klaw.com
wmp@cpuc.ca.gov
wtr@cpuc.ca.gov
xbaldwin@ci.burbank.ca.us
zaf@cpuc.ca.gov

TGlassey@Certichron.com
tien@eff.org
tjs@cpuc.ca.gov
tmfry@nexant.com
tomk@mid.org
tpomales@arb.ca.gov
traceydrabant@bves.com
trh@cpuc.ca.gov
ttutt@smud.org