VCC OUTLINE – KEY ELEMENTS

Note: This document was developed as an initial starting point for the VCC Multistakeholder Process discussions. It is not intended to be a final or exhaustive list, but it is expected that it will be further refined and edited by stakeholders participating in the process.

1. **MANAGEMENT AND ACCOUNTABILITY – Elements that relate to the credibility of the utility and/or third party's privacy function.**
    - Identify a privacy officer[1,2,3,4]
    - Perform a risk assessment[1,3]
    - Conduct independent audits[1,2,3,5,6]
    - Perform a Privacy Impact Assessment[2]
        - Determine risk[1,3]
        - Evaluate protections[1]
        - Verify compliance with legal, regulatory and policy requirements
    - Address employee access[2,4]
        - Develop policies for employee access
        - Develop policy for handling terminated employees
    - Describe employee training[1,2,3,6]
        - Background checks
        - Information handling
        - Collections
    - Describe how privacy policies will be communicated to the consumer
        - Short form versus long form

2. **NOTICE AND PURPOSE – Elements that relate to communicating applicable policies, and related choices, to customers.**
    - Outline customer rights for accessing this information[8]
    - Identify the types of data covered by the VCC[8]
        - Energy use data
        - Personally identifiable data
        - Explicitly state what data is being shared
    - Define procedure for complaint resolution[1]
    - Specify how consumers will be notified of VCC (organizational participation)

3. **CHOICE AND CONSENT – Elements that relate to the customer's granting of authorization for the release/sharing of his or her data.**
    - Consumers should have the ability to share with third parties[2]
    - Specify at what point consent must be obtained[7]
        - Time of use/collection or as standard utility privacy policy
        - For each third party
    - Identify methods of consent[5]
        - Management of this process
        - Electronic, paper form, etc.

- Consider time and effort required for consumer to give consent[1]
    - Process should be clear, concise, understandable, accessible[1,3,6]
- Specify time period for consent/expiration[6]
    - Reauthorization procedures including revisions to policy[1,3]
- Define disclosure practices
    - Clearly explain who will have access to the data with the obtained consent[8]
        - Affiliates, agents, subsidiaries
- Outline time parameters for using data once consent is given
- Identify methods of withdrawal
- Consider ease of withdrawal/cancelation of authorization[1,6]
- Specify reasons for cancelation and time period to take effect
- Define how the data will be used once collected[8]
- Notify individuals about the use of their data[5]
    - Includes proposed changes in use of data
- Define access points[1,7]
    - One way to organize this information is through privacy use cases[1,3]
- Define who will have access to the data[3,5]
- Specify who has the responsibility for validating consent

4. **COLLECTION AND SCOPE – Elements that relate to the scope of customer data that is collected, and potentially shared.**
    - Specify terms and conditions for consent[1]
    - Outline reasons for collecting data[2,8]
    - Data collection should be limited to only the necessary information to accomplish the purpose/task[1,3,5]
    - Identify what data is being transferred

5. **USE AND RETENTION – Elements that relate to how long customer data should be kept, and when it should be destroyed.**
    - Describe data retention and disposal[1,3,5,6]
        - Specify how long data will be retained[1]
        - Define process for handling data
        - Define method for disposal of data[3]
    - Define how retention policy will function in the case of mergers and acquisitions[1,8]
    - Define who has access without consent
        - Agents
        - Contractors
        - Law Enforcement

6. **INDIVIDUAL ACCESS – Elements that relate to the customer accessing his or her own data.**
    - Consumers should have access to their data2,4
        - State unequivocal consumer right to access[2,4,5,6,8]
    - Describe options for receiving data[1]

7. **DISCLOSURE AND LIMITING USE – Elements that relate to how customer data is shared with third parties**
    - State goals of data minimization[3,5,6]
    - Define limits of third party data sharing practices[7]
    - Define the requirements for aggregated and anonymized data[7]
    - Require commitment from entities with access to aggregated and anonymized data not to reverse engineer data[1,3,8]
    - Define conditions/parameters for researcher access
    - Define parameters for access to whole building data for submetered buildings

8. **SECURITY AND SAFEGUARDS – Elements that relate to how customer data should be protected from un-authorized disclosure.**
    - Describe data security methods
    - Protect data against loss, unauthorized use, modification, etc.[1,3,5]
    - Define a process for handling breaches[3,8]
    - Define how customers will be notified of breaches[2]
    - Define who is responsible for data breach notification and remedies of breaches

9. **ACCURACY AND QUALITY – Elements that relate to the maintenance of accurate and complete customer data.**
    - Endorse data quality[1,2,3,6]
        - Consumers should expect quality data[1,6]
    - Identify procedure for correcting inaccuracies
        - Consumers should be able to obtain corrections to inaccuracies[2,3,6]

10. **OPENNESS, MONITORING, AND CHALLENGING COMPLIANCE – Elements that relate to customer education and complaints.**
    - Provide customer education and awareness[1,3]
    - Develop a mechanism for handling complaints[1,3,6]

11. **ENFORCEMENT MECHANISMS[5]** (not addressed in NAESB nor the NISTR)
    - Define consequences for noncompliance[5]

12. **POTENTIAL GLOSSARY/DEFINITIONS**
    - Aggregated Data
    - Anonymized Data
    - Authorization[1]
    - Behavioral Information[2]
    - Confidential[2]
    - Contracted Agent[3,4,6]
    - Contractors[2]
    - Customer/Consumer Energy Usage Data[3,6]
    - Customer[3,6]
    - Internal Information[2]

- NAESB
- Personally Identifiable Information[2]
- Primary purpose[4,6]
- Privacy Use Case[1,3,6]
- Private Customer Information[2]
- Public Information[2]
- Secondary purpose[4,6]
- Smart Meter-based Information[1]
- Third party[1,2,3,4]
- Vendors[2]

OTHER ITEMS FOR CONSIDERATION

Management of VCC

- Process for updating code[8]
- Maintenance of lists of VCC adopters[7]

Ownership of VCC

- Characteristics of owner organization[8]

Implementation Cost[5,8]

- Cost associated with sharing data in general, distinguished from additional costs or savings of privacy implementation

Endnotes

[1]REQ 22. North American Energy Standards Board (NAESB), August 8, 2011. http://www.naesb.org/member_login_form.asp?doc=retail_bk22_043012.pdf
[2]"A Model Privacy Policy for Smart Grid Data." Vermont Law School, Institute for Energy and the Environment, accessed January 11, 2013. http://vermontlaw.edu/Documents/Model%20Smart%20Grid%20Privacy%20Policy%20VLS%20Version%202.pdf
[3]"Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties." Smart Grid Interoperability Panel, Cyber Security Working Group (CSWG), August 13, 2012. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/Third_Party_Privacy_Best_Practices_Document_v4_Final.pdf
[4]Xcel Energy Filing to the Minnesota Public Utilities Commission. March 5, 2012. https://www.edockets.state.mn.us/EFiling/edockets/searchDocuments.do?method=showPoup&documentId={B9935C53-8004-4EC3-9F89-D6DE8DCF1C09}&documentTitle=20123-72239-01
[5]"A Regulator's Privacy Guide to Third-Party Data Access for Energy Efficiency." State and Local Energy Efficiency (SEE) Action Network, December 2012. http://www1.eere.energy.gov/seeaction/pdfs/cib_regulator_privacy_guide.pdf
[6]"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 and Electric Company." July 28, 2011. http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf
[7]Suggested by the Federal Smart Grid Task Force (SGTF). December 2012 – January 2013.
[8]Suggested by stakeholders at the preliminary voluntary code of conduct (VCC) meeting. December 17, 2012.