DOE VCC Integrity and Security Workgroup

Proposed Principles

Category 1: Security and Safeguards

1. Data Security Methods	
Proposed Principle:	
Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, related entities and customers.	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o Implement technical, process and administrative controls (including plans and procedures) that are reasonably designed to address existing and foreseeable threats to the confidentiality, integrity, and availability of the operations technology (OT) and information technology (IT) assets, as well as the data which these systems process or store. o Such controls should address both external and internal threats, including employees, vendors and partners. o Responsibility for controls management should extend to the technology, risk, procurement and vendor management; compliance, legal and audit groups with oversight by executive management; and the board of directors, if there is such. o Incorporate data security and privacy protection into contracts or agreements with vendors, partners and other third parties.

2. Data Protection Against Loss, Unauthorized Use, Modification, etc.	
Proposed Principle:	
"**Implement and maintain process, technology, and training measures to ensure data integrity and protect against loss and unauthorized use, access or dissemination**."	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o Record and identify access to or movement of CEUD or Account Data consistent with the sensitivity of the data, appropriate business purpose, and technical complexity of the systems. o Create and manage identities for entities that may be granted logical or physical access to the organization's assets. o Support data integrity and confidentiality through maintenance of a comprehensive record retention program for sensitive or critical data with designated data owners. o Implement appropriate technical controls, such as encryption, for data at rest and in transmission. o Ensure that all authorized users receive formal training for use and handling of data, and that appropriate administrative measures are instituted for noncompliance.

3. Define Process for Handling Data Breaches	
Proposed Principle:	
Maintain a comprehensive breach response program for the identification, containment, mitigation and resolution of any incident that causes or results in the breach of data security.	
References	**Examples and Explanatory Implementation Guidance**

• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o The program should include all relevant internal stakeholders (e.g., technology, security, legal, privacy regulatory relations, corporate communications), as well as a process for involving external entities such as law enforcement agencies and/or incident coordination groups (e.g. ICS-CERT, etc.). o It should also include a process for documenting root causes, implementation of remedial measures, and recording lessons learned from the event.

4. Define Process for Customer Notification of Data Breaches	
Proposed Principle:	
Customers should be notified when it is reasonably likely that their personal information has been accessed without authorization under circumstances which may result in misuse of CEUD or Account Data. [Note: Coordinate with Notice/Awareness Group]	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o Notice should occur within a reasonable period of time after the nature and extent of the breach is determined. o Such notice should inform the customer of the circumstances surrounding the breach, the information about them which may have been affected, what they can or should do to protect themselves against misuse of the information by others, and the steps which have been taken to preclude future, similar events. o The notice should be delivered in a manner consistent with other means by which the customer is advised of significant actions which may affect them, such as changes in policy, delivery of goods or services, or pricing. [Data breach notification: Coordinate with Notice/Awareness group]

5. Define Responsibility for Data Breach Notification and Remedies	
Proposed Principle:	
The Service Provider whose customer's information may have been compromised has the primary responsibility for ensuring the delivery of complete, accurate and timely notice to the customer and remedying the conditions which led to the breach. [Coordinate with Notice/Awareness Group]	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o "Service Provider" refers to the utility or third party that has adopted the Voluntary Code of Conduct, and whose customer's information may have been compromised, regardless of whether the compromise occurred through the Service Provider itself or through a vendor. o The Service Provider may require, by contract or other agreement, that the entity (e.g., vendor) having actual responsibility for the breach will deliver the notice. However, this must be done in a way that does not confuse the recipient of the notice as to the identity of the Service Provider to whom they originally disclosed the personal information.

Category 2: Data Quality and Accuracy

1. Data Quality	
Proposed Principle:	
Account Data and CEUD should be reasonably accurate and complete, considering the circumstances and environment in which it has been collected (e.g., validated data, data collected indirectly from another entity, etc.). When a Service Provider has modified or enhanced data that it initially received from another source (e.g., a utility or a different third party), the customer receiving the enhanced or modified data should generally be made aware that such data may differ from the initial data.	
References	**Examples and Explanatory Implementation Guidance**
• NAESB REQ 22. North American Energy Standards Board (NAESB), August 8, 2011. http://www.naesb.org/member_login_check.asp?doc=retail_bk22_043012.pdf • NIST 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 • California PUC Rules. 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 • Vermont Model Privacy Policy: 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	o An authorized third party asks for real-time, 15 minute interval data from a customer's smart meter. Assuming the utility is capable and willing to provide such data, the utility should give the party as reasonably accurate and complete data as is practicable, recognizing that the utility has not had an opportunity to validate the data, and there may be "pings" or "blips" that have not yet been corrected. o An authorized fourth party asks for customer data from a third party, who had previously obtained it from a utility. The third party should endeavor to provide as reasonably complete and accurate data as it can, recognizing that the data it provides can only be as accurate and complete as the data it originally obtained. o A third party collects customer data from a utility. It then modifies or enhances the data with other information, analysis, etc. If the third party then discloses that data to another party, it should communicate that it has enhanced or modified the data, such that it is different than the data originally received from the utility.

2. Data Accuracy	
Proposed Principle:	
• **Utilities and third parties should provide a process for customers to dispute the accuracy or completeness of their own Account Data or CEUD, and to request appropriate corrections or amendments. Existing procedures for addressing other types of customer complaints may be adequate.** [Note: Coordinate with Management / Redress working group.]	
References	**Examples and Explanatory Implementation Guidance**
• NAESB REQ 22. North American Energy Standards Board (NAESB), August 8, 2011. http://www.naesb.org/member_login_check.asp?doc=retail_bk22_043012.pdf • NIST 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 • California PUC Rules. 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 • Vermont Model Privacy Policy: 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	o A customer receives a bill from the utility and notices that the bill included the wrong Account Data (email address, account number, rate class, etc.). A process should be available to the customer to contact the utility and correct the mistake. A separate "Customer Data" process may not be necessary if a general customer compliant hotline or other process is sufficient. o An authorized third party provides a service to the customer using the customer's Account Data or CEUD as collected from the utility (and possibly enhanced or modified). In reviewing the third party's product, the customer realizes there is a mistake in his or her CEUD or Account Data. The third party should have a process available to the customer to correct the mistake or, if applicable, determine that the mistake was contained in the original data.

Next Steps: Coordinate with other groups after November 22nd face-to-face meeting as noted above in highlighted brackets.