Department of Energy Voluntary Code of Conduct
Integrity / Security Workgroup

I. Areas of Consensus

Topic	*Subtopic*	*Proposed Principle*	*Reference/ Notes*
Data Security Methods	Describe data security methods.		See conflict/inconsistencies
	Describe data security methods.	The bolded part is integrity/security related. The personnel part should be related to management/redress.	**NAESB REQ.22.3.1.1.1** Distribution Companies **should have internal information security and privacy policies and practices** relating to the disclosure of Smart Meter-based Information to Third Parties and should have personnel appointed to a position responsible for compliance with such policies and practices.
			NAESB REQ.22.3.8.1.1 Distribution Companies should protect Smart Meter-based Information under its control from unauthorized access and disclosure by developing and incorporating information privacy protections, as they relate to the disclosure of Smart Meter-based Information to Third Parties, into their policies and practices.
			NAESB REQ.22.3.8.2.1

			Third Parties should protect Smart Meter-based Information under its control from loss, theft, unauthorized access or disclosure, unauthorized copying, misuse, or modification by developing and incorporating information privacy protections into their Smart Meter-based Information policies and practices.
			NIST: Data Security & Governance Third Parties should protect information under their control from unauthorized access, copying, modification, inappropriate disclosure, or loss by having information privacy protections in policies, procedures, and practices relating to data security and to 166 disclosure and accuracy of data disclosed to the Third Party's Contracted Agents, or to other Third Parties. These policies or procedures should periodically be reviewed, assessed, and updated, as necessary, to ensure CEUD is properly

			addressed.

Topic	***Subtopic***	***Proposed Principle***	***Reference/ Notes***
Data Protection	Protect data against loss, unauthorized use, modification, etc.		See conflict/inconsistencies
	Protect data against loss, unauthorized use, modification, etc.	bolded relevant parts	**NAESB REQ.22.1.7** A Third Party seeking or provided Smart Meter-based Information should be an identifiable Entity that is permitted to receive Smart Meter-based Information **in accordance with** the Governing Documents and the requirements of the Applicable Regulatory Authority, **including applicable cyber security and privacy requirements.**
			NAESB REQ.22.3.1.1.3 Distribution Companies should internally audit and monitor their own Smart Meter-based Information activities that relate to the disclosure of Smart Meter-based Information to Third Parties.
			NAESB REQ.22.3.1.2.3 Third Parties should

			audit and monitor their own Smart Meter-based Information activities (e.g., collection, access, use, retention, disclosure, etc.).
			NAESB REQ.22.3.1.1.5 The Distribution Company should **establish and implement a process designed to prevent its terminated employees from obtaining unauthorized access** to the Smart Meter-based Information that is within the control of the Distribution Company.
			NAESB REQ.22.3.1.2.5 The Third Party should **make reasonable effort to prevent its terminated employees from obtaining unauthorized access** to the Smart Meter-based Information that is within the control of the Third Party.
			NIST: Employee Training Third Parties and Third Party's Contracted Agents should develop, disseminate, and 216 periodically review and update a **formally documented security and privacy awareness and training**

			policy (which specifically includes the protection of CEUD) with documented supporting implementation procedures. The organization should **document, maintain, and monitor each employee's security and privacy training activities** on an individual basis, including basic security and privacy awareness training in accordance with the organization's security and privacy policies.
			NIST Audits Each Third Party should conduct a **periodic independent audit of Third Party's data privacy and security practices**. Each Third Party should **periodically verify the privacy and security practices** of Third Party's Contracted Agents. This may occur in one or more ways. Some examples are: 1. Conducting an audit of the Third Party's Contracted

			Agents' privacy and security practices. 2. Requiring the Contracted Agent to provide Third Party with an independent audit of its privacy and security practices. 3. Examining the results of an independent audit of the Third Party's Contracted Agents' privacy and security practices. 4. Examine the results of a recent SSAE-16 audit. 5. Review any existing Information Security Management System (ISMS) certifications. 6. Review any recent privacy impact assessments that have been performed.

Topic	***Subtopic***	***Proposed Principle***	***Reference/ Notes***
Data Breaches	Process for Handling Breaches Breach Notification Responsibility for Data Breach notification and		See conflicts/inconsistencies

	breach remedies		
			NAESB REQ.22.3.8.1.2 In the event of any Distribution Company-confirmed breach of the security of a system under a Distribution Company's control that results in the unauthorized access to and disclosure of Smart Meter-based Information, a Distribution Company **should comply with applicable requirements and laws, including any Retail Customer notification requirements**, pursuant to the Governing Documents and the Applicable Regulatory Authority rules and regulations. The Distribution Company should **restore the integrity of the system** and data to the extent and as soon as reasonably practicable.
			NAESB REQ.22.3.8.2.2 In the event of any breach of the security of a system under a Third Party's control that results in the unauthorized disclosure of Smart Meter-based Information, a Third Party **should comply with**

			applicable requirements and laws, including any Retail Customer notification requirements, pursuant to the Governing Documents and the Applicable Regulatory Authority rules and regulations. The Third Party should **restore the integrity of the system** and data as soon as and to the extent reasonably practicable.
			NIST: Data Breaches Third Parties should **identify any state or federal requirements for disclosure or data breach notification** that may be applicable to a Third Party or Contracted Agent. **Consider including CEUD as data that may require a notice for any unauthorized breach** dependent upon the granularity of the data and applicable legal breach notification requirements.

Topic	***Subtopic***	***Proposed Principle***	***Reference/ Notes***
Data Quality	Consumers should expect quality data. Procedures for consumer to obtain corrections for	- Organizations should ensure that the data is accurate and as complete as possible. - Organizations should provide a reasonably clear and easy method for customers to	See conflicts/inconsistencies

	inaccuracies	address perceived discrepancies in the data.	
			NIST: Customer Access to Their Data A Third Party should develop and communicate processes for a Customer to have access to their CEUD and to be able to request that the CEUD be corrected where inaccuracies exist. The process for gaining data access should be a relatively simple process for the typical Customer. This process, which may include existing procedures established or approved by the applicable regulatory authority or other legal requirements, should be discussed in the notices to the Customer. The data provided to the Customer should be provided in a form that is reasonably understandable by the average Customer. **Customer Authorization & Data Accuracy** Third Parties should provide Customers with reasonable mechanisms for: 1. granting and revoking authorization for access to their

			CEUD; 2. providing feedback regarding the disclosure of CEUD; and 3. requesting corrections to the CEUD.
		-	**NIST: Data Quality** Third Parties and Third Party's Contracted Agents using CEUD should endeavor to ensure that the data is accurate and complete. It should be recognized that the data is only as accurate and complete as the information received if the holder is not the original collector. This should not preclude a Third Party or Third Party's Contracted Agents from modifying or enhancing CEUD, provided that it is clear that modifications or enhancements have been made when such information is disclosed.

II. Areas of Conflict/Inconsistencies

Topic	*Subtopic*	*Majority Position*	*Minority Position*	*Reference/ Notes*
Data Security	Describe data		**Only the CDP deals with data**	

Methods	security methods.		**security methods – all of the other documents are silent or only make passing references to the need for security methods.** SECURITY: Consumers have a right to secure and responsible handling of personal data. Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure (CDP). The Security principle recognizes these needs. It gives companies the discretion to choose technologies and procedures that best fit the scale and scope of the personal data that they maintain, subject to their obligations under any applicable data security statutes, including their duties to notify consumers and law enforcement agencies if the security of data about them is	

			breached, and their commitments to adopt reasonable security practices. (CDP)	
	Describe data security methods.	In these 3 documents, there are different approaches: 1. NISTIR 7628 Vol. 1's High-Level Security Requirements go into great detail about what methods to use to secure data in a system. There is also a recommendation in Vol. 2 to use privacy use cases and privacy risk assessments when determining appropriate protections. 2. NAESB REQ.22 only addresses the use of privacy risk assessments and privacy use cases when determining appropriate protections. 3. In Colorado 723-3, it is stated that it is expected all utilities, market participants, and Interconnection Customers interconnected with electric systems to comply with the recommendations offered by the President's Critical Infrastructure Protection Board and best practice recommendations from the electric reliability authority. All public utilities are expected to meet basic standards for electric system infrastructure and operational security, including physical, operational, and cyber-security practices.		For determining particular methods, I would recommend pointing to readily available documents regarding risk assessments and security requirements that organizations could utilize in developing their data security methods.
Data Protection	Protect data against loss, unauthorized use, modification, etc.	In general, all of the documents express directly or indirectly a desire to protect consumer data but there are strong inconsistencies, particularly when it comes to energy data.	**The biggest area of conflict comes in with third party data. Some of the policies (pasted below) assume that third parties will gain access to the data without consumer authorization while the DAP states that no third party should gain access to utility customer data without prior affirmative consent.**	All classes of electric utility customers should be entitled to protect the privacy of their own individual energy-usage data including commercial enterprises.(sap)

			Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise (cdp) ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their	

			performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise. (cdp) Utilities should not disclose CEUD to third parties unless a given consumer has consented to such disclosure affirmatively, through an opt-in process that reflects and records the consumer's informed consent.(Dap) Second, jurisdictions designing such opt-in authorization processes should require a valid authorization that specifies the purposes for which the third-party is authorized to use CEUD, defines the term during which the authorization will remain valid and identifies the	

			means through which consumers can withdraw such authorizations.(DAP) Third, third parties authorized to receive CEUD should be required to protect the privacy and the security (including integrity and confidentiality) of CEUD that they receive and to use it only for the purposes specified in the authorization.(DAP) Fourth, States should enact laws or rules that define the circumstances, conditions, and data that utilities should disclose to third parties(DAP)	
	Protect data against loss, unauthorized use, modification, etc.	Data should be protected against loss, theft, unauthorized access, disclosure, copying, misuse, or modification. (NISTIR 7628 Vol. 2 and NAESB REQ.22.3.8.2.1)	"Distribution Companies should protect Smart Meter-based Information under its control from unauthorized access and disclosure …" NAESB REQ.22.3.8.1.1 "A utility shall provide … access to the customer's standard customer data … in a manner that ensures adequate protections for the utility's system security and the continued privacy of the customer during transmission." CO 723-3 §3026 (c) and (d)	Distribution Companies have less protections necessary than Third Parties in NAESB REQ.22. The list of protections required of Third Parties matches the list from NISTIR 7628 Vol. 2. There are also more types of protections required in Vol. 1's High-Level Security Requirements. Colorado's language implies protecting against

				unauthorized access, but is too general to assume much else.
Data Breaches			**Data breaches are only discussed in the CDP document.** Supports creating a national standard under which companies must notify consumers of unauthorized disclosures of certain kinds of personal data in replace the multiple state and territory level Security Breach Notification laws. (CDP)	
	Process for Handling Breaches	There are different approaches: 1. NISTIR 7628 states that an organization should have policies in place for how to handle a breach. 2. NAESB REQ.22 states that any applicable requirements from laws, any Retail Customer notifications requirements, pursuant to the Governing Documents and the Applicable Regulatory Authority rules and regulations should be followed. 3. Colorado 723-3 does not seem to deal explicitly with this topic. There may be guidance from the President's Critical Infrastructure Protection Board and best practice recommendations from the electric reliability authority that is applicable.		
	Breach Notification	1. NISTIR 7628 says that an organization should have procedures in place for notifying the affected individuals in a timely manner with appropriate details. 2. NAESB REQ.22 says that any Retail Customer notifications requirements, pursuant to the Governing Documents and the Applicable Regulatory Authority rules and regulations should be followed.		

		3. Colorado 723-3 does not seem to deal explicitly with this topic. There may be guidance from the President's Critical Infrastructure Protection Board and best practice recommendations from the electric reliability authority that is applicable.		
	Responsibility for Data Breach notification and breach remedies	1. NISTIR 7628 deals with breach remedies in the Access Control, Incident Response, and the System and Communication Protection families of high-level requirements in Vol. 1. 2. NAESB REQ.22 says that an organization should restore the integrity of the system and data to the extent and as soon as reasonably practicable. 3. Colorado 723-3 does not seem to deal explicitly with this topic. There may be guidance from the President's Critical Infrastructure Protection Board and best practice recommendations from the electric reliability authority that is applicable.		
Data Quality	Consumers should expect quality data. Procedures for consumer to obtain corrections for inaccuracies		**Only CDP and DAP contain discussion of methods for ensuring data accuracy and quality and methods for fixing inaccuracies.** Consumers have a right to easily understandable and accessible information about privacy and security practices. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear	

			descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties. (CDP) Privacy notices that distinguish personal data uses along these lines will better inform consumers of personal data uses that they have not anticipated, compared to many current privacy notices that generally give equal emphasis to all potential personal data uses.20 Such notices will give privacy-conscious consumers easy access to information that is relevant to them. (cdp) ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to	

			consumers if the data is inaccurate. Companies should use reasonable measures to ensure they maintain accurate personal (cdp) On this question, almost all proponents of both consumer-ownership rights and consumer-access rights agree: Consumers should decide whether and for what purposes any third-party should be authorized to access or receive CEUD (DAP) Consequently, consumers should have rights to protect the privacy of their own CEUD and control access to it. Well designed implementations of Smart Grid technologies should also empower individual consumers to make a wide array of choices about whether or how to manage their own energyconsumption data via home energy management systems.data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the	

			appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm. (dap) Each app shall state whether it shares user-specific data with any category of third party entity that falls within any of the following: • Ad Networks (Companies that display ads to you through apps.) • Carriers (Companies that	

			provide mobile connections.) • Consumer Data Resellers (Companies that sell consumer information to other companies for multiple purposes including offering products and services that may interest you.) • Data Analytics Providers (Companies that collect and analyze your data.) • Government Entities (Any sharing with the government except where required or expressly permitted by law.) • Operating Systems and Platforms (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.) • Other Apps (Other apps of companies that the consumer may not have a relationship with.) • Social Networks (Companies	

			that connect individuals around common interests and facilitate sharing.) App developers shall not be required to disclose sharing with third party service providers where a contract between the app and the third party explicitly: (i) limits the uses of any consumer data provided by the app to the third party solely to provide a service to or on behalf of the app; and, (ii) prohibits the sharing of the consumer data with subsequent third parties.User-specific data does not include aggregated information that does not include any of the user's personally identifying information, and would not allow that information to be inferred.(NTIA)	
Information Sharingby Stakeholders	Web portal or library should be developed		**The DAP and SGP recommend creating centralized resources, such as a library or web portal, for privacy and data protection policies.** To promote further cooperation and dissemination of information	

			about practices relating to the regulation of the privacy and data-protection aspects of smart-grid technologies, a web portal should be created to act as a "clearinghouse" for such data. (DAP) Develop and compile an information library of ongoing activities that can be used and accessed by all Stakeholders. (SGP)	