**via posting**

**DATE:** August 6, 2019

**TO: Board Digital Committee:** Dick Brooks, Jim Buccigross, Cade Burks, Valerie Crockett, Michael Desselle, Howard Gugel, Steven McCord, Annie McIntyre, Joelle Ogg, Randy Parker, Emil Pena, Timothy Simon, Leigh Spangler, Terry Thorn, Sue Tierney, Pat Wood

**FROM:** NAESB Office

**RE:** Draft NAESB Board Digital Committee Survey Results

Dear Digital Committee Members,

Thank you for your participation in the Board Digital Committee’s efforts to develop a report concerning the digitalization of the energy industry and how it may impact NAESB. The survey sent to you on July 26th and the results of the survey are included below. As previously discussed, the information provided will be reviewed during our call on August 8th, and we will determine if there is any additional information that should be collected and included in the next iteration of the report.

With Best Regards,



Jonathan Booe

Executive Vice President & Chief Administrative Officer

North American Energy Standards Board

| **NAESB Digital Committee Survey Results** |
| --- |
| **Q1: For Distributed Ledger Technology, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define Distributed Ledger Technology?** |
| This is an immature field with terminology still evolving and with numerous “working definitions” – none universally recognized. Definitions from frequently referenced sources do not agree (e.g., Gartner, NIST, Wikipedia, etc.). Numerous Blockchain/DLT related articles and reports have definitions within the context of the document, but do not necessarily “fit” beyond that context. A set of NAESB “agreed upon” definitions for the Energy Industry is a definite need and would be most useful. Candidate terms to define: Distributed Ledger, Blockchain (as a variant of DL), and Smart Contract. Current TVA internal definitions:  1. Blockchain/Distributed Ledger Technology (February 2019): A distributed data management protocol utilizing ledger technology for ordering, validating, and maintaining records of digital asset transactions in a consensus-based immutable manner.  2. Smart Contract (February 2019): A collection of if/then statements codified in a digital protocol that self-execute on predefined criteria and thus represents traditional contract processes, including contract formation, creation of enforceable and immutable rights and obligations, and execution of performance. |
| Not currently applicable |
| Transaction processing across a secure distributed network |
| The use of data blocks to validate a transaction and mine transactional data. |
| A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies. It allows transactions to have public "witnesses," thereby making a cyberattack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. |
| Using shared ledger files maintained across multiple computers on multiple networks to maintain data integrity/security. To the best of my knowledge, TransCanada Pipelines Limited is not currently using the technology. |
| **Are there any (additional) use cases / business cases for the technology that should be considered?** |
| Beyond the current NAESB efforts on Natural Gas post-trade settlement processing, any Energy Industry use case that aligns to these criteria from Gartner would be good candidates for a DLT-based solution – read as a set of conditions that must exist for a good use case:   1. Consistent data store across multiple entities, 2. Tamper-proof log of all wit4es to the data store, 3. Data records once written are never modified or deleted, 4. More than one entity contributes to the data, 5. Entities with write-access have a hard time deciding who should be in control of the data store, and 6. Shared visibility and history, and high availability for shared data.   Numerous use cases align with the utility value chain: Generation (including Traditional & Renewables), Market Operations and Trading, Transmission, Distribution, Consumer & Prosumer (selling excess energy back to the grid). Typical use case categories include:   1. Wholesale Markets (energy trading/settlement; Carbon Credits and Renewable Energy Credits), 2. Decentralized Generation & Grid Management (Grid, DER, and Smart Home), 3. eV Charging & Mobility (energy source provenance; access and settlement management), 4. Peer-to-Peer (P2P) (prosumer to consumer), 5. Retail Switching & Retail Market Settlements, 6. Payment Enablement (currencies & tokens), 7. Operations & Efficiencies (streamlined operations & back office processes), 8. Security Management (for participants and devices). |
| Energy trading, invoice payments |
| Focus on blockchain in permissioned networks (other implementations offer anonymity and other attributes less useful in the transaction space). |
| NAESB's EIR would be a good use case for distributed ledger technology |
| This overview from NIST lists active standards efforts … <https://csrc.nist.gov/CSRC/media/Presentations/NIST-Block-Chain-Research-Project/images-media/ar-dy-blockchain-combined.pdf> |
| **What are the benefits of adopting the technology?** |
| Paramount is improving our enterprise capabilities with DLT/Blockchain as a key enabling technology that:   1. Is “broadly applicable” to our Core (Energy, Environment, and Economic Development) and Corporate (Supply Chain, Finance, HR, etc.) functions, 2. Provides “connected trust” enabling individuals, organizations, devices, machines, algorithms (and combinations) to conduct business in more direct and efficient ways, 3. Is “potentially transformative” through opportunities to re-think how energy is supplied and consumed, how assets are validated, and how business is conducted.   Key benefits we expect:   1. Increased data & process transparency, 2. Reduced operational & administrative costs, 3. Accelerated operational & administrative processes, 4. Enhanced security & trust, and 5. Improved standardization. |
| Reduced errors, faster processing |
| Offers a fairly easily implemented, secure method of transacting and traceability. |
| Eliminate single points of failure and make information shareable in a distributed fashion |
| Provides a level of trust and security in shared files. |
| **What are the costs/issues/concerns associated with the adoption of the technology?** |
| 1. Much “hype” as an emerging tech - Still immature as far as mainstream adoption; utilities “lag” with respect to Financial and Supply Chain sectors, 2. Standards & Regulations - Evolving and don’t yet adequately address needs; inconsistent, 3. Legal perspective - Smart contracts recognition and enforcement; Federal and State laws evolving; inconsistent, 4. Culture Resistance - Companies accustomed to “central authority”, 5. Production Scale? - Many Proof-of-Concept and Pilots…where is the mainstream Production Scale evidence, 6. Industry “Tension” - Competition; comfort with data sharing; buy-in for Industry-wide Use Cases – how many in an industry need to “agree” to develop a DLT-based solution and be considered representative/inclusive; who will fund and who will get benefits; collection of fees/transaction, coverage for admin overhead, 7. Knowledge & Talent - Lack of applied/practical knowledge in both technical and managerial ranks; small, but growing talent pool, and 8. Technology “Switch-Over” - Time and costs to move from existing “legacy” systems; questions about “proof-of-value” over existing systems. |
| Mostly confidentiality, and of course security |
| Ensuring that $ are focused on an implementation that will be standardized and accepted in the industry. |
| Unauthorized access to sensitive information that could be placed on a DLT |
| **Are there other standards development efforts that the committee should monitor?** |
| General Industry: These groups have efforts in progress to address standards for general industry:   1. The Enterprise Ethereum Alliance (EEA), 2. The Linux Foundation Hyperledger open source collaborative effort, 3. National Institute of Standards and Technology (NIST), 4. Institute of Electrical and Electronics Engineers (IEEE), 5. American National Standards Institute (ANSI), 6. International Organization for Standardization (ISO), 7. World Wide Web Consortium (W3C), 8. Internet Research Task Force (IRTF), 9. International Telecommunications Union (ITU), and 10. Medium.com writer James Barry about Blockchain Standards - series of “insightful” articles.   Energy Industry: These blockchain “groups” have significant Energy Industry membership and should be considered for standards engagement:   1. Energy Blockchain Consortium, 2. Energy Web Foundation (EWF), 3. Electric Power Research Institute (EPRI), 4. New York Utilities Group. |
| <https://www.oasis-open.org/committees/download.php/62905/Unbound%2520KMIP%2520Presentation%2520RSA%25202018.pdf> |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| DLT/Blockchain is but one item in a broad perspective to consider around Technology Disruptors in the Energy sector. Look to “Future of Energy” type publications/presenting to identify other disruptors that align and mutually enable/benefit each other (e.g., DLT and IoT). |
| Despite several reviews/meetings on DLT, we still lack a clear use case in the energy trading space |
| Data standardization is a critical first step in the decision to use DLT. The data that's placed on a DLT should be agreed by all parties that plan to implement a DLT. |
| **Q2. For the Internet of Things, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define the Internet of Things?** |
| TVA’s broadest definition, which encompasses consumer as well as industrial technology: The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. TVA has adopted the Industrial Internet Consortium (IIC) definition for industrial IoT technology: An Industrial Internet of Things (IIoT) system connects and integrates industrial control systems with enterprise systems, business processes and analytics. TVA acknowledges that both consumer and industrial IoT technologies are at play in our lower risk environments. |
| Not currently applicable |
| The enabling or enhancement of otherwise "unconnected" processes or objects via the Internet |
| Connectivity of distributed digital assets that offers central command and control. |
| Tools and Techniques that provide operational entities with useful information to support real-time situational awareness and decision making. |
| Technology that allows connected physical devices to communicate with and/or control each other over the internet. Most common example is that of connected smart devices in homes. |
| **Are there any (additional) use cases / business cases associated with the Internet of Things that should be considered?** |
| Near term:   1. Condition Based Maintenance, 2. Reliability and Outage Optimization, 3. Enhanced Situational Awareness and Decision Support, 4. Advanced Metering Infrastructure (AMI), 5. Smart Facilities, Equipment, and Instrumentation, 6. Fleet and Asset Management Optimization, 7. Enhanced Physical Security.   Longer term:   1. Predictive Maintenance, 2. Generation Optimization, 3. Smart Grid, Microgrids, Energy Storage Infrastructure, 4. Continuous Environmental, Health, and Safety Monitoring, 5. Autonomous Operations, especially DER Infrastructure, 6. Electric Vehicle Infrastructure. |
| IOT would seem to have most usefulness in the SCADA/control environment |
| IoT is gaining traction in the operational space, even in high consequence areas (i.e. process safety) |
| Monitoring and sensing for Distributed Energy Resources |
| I am not aware of any as they may relate to NAESB Standards. There could be some back-office applications. |
| **What are the benefits of adopting technology that supports the Internet of Things?** |
| 1. Lower Costs, 2. Optimized Assets, 3. Conserved Resources, 4. Responsive and Efficient Operations, 5. Improved Reliability, 6. Improved Awareness and Ability to Act- When coupled with real-time AI and Data Analytics, 7. Improved Safety and Security, 8. Improved Compliance, 9. Lower Risk.   #7,8 & 9 if implemented and operated securely, which is a current challenge. |
| Increased visibility and response times |
| Increased situational awareness in a networked environment, rapid response, remote control. |
| Situational awareness from grid edge devices to improve real-time decision making by controlling entities |
| Potentially lower cost than traditional communication methods. |
| **What are the costs/issues/concerns associated with the adoption of the technology?** |
| 1. Immature IoT/IIoT Standards, Laws, and Regulations, 2. Immature supporting elements such as software, interoperability protocols, AI, data governance, and analytics, 3. Lack of adoption and requirement for adoption of existing standards by manufacturers, 4. Lack of integrated system, information, and business process perspective, 5. Lack of cyber and asset management basic hygiene for existing deployed IoT elements, and 6. Relative lack of Cyber Physical Security expertise overall. |
| Security, security, security |
| IoT greatly increases an attack surface and can introduce significant cyber security risks. |
| Cybersecurity is #1. IoT data must be trustworthy in order to be useful. |
| Management, secure communications, and security of the devices |
| **Are there other standards development efforts that the committee should monitor?** |
| 1. National Institute of Standards and Technology (NIST), 2. National Renewable Energy Laboratory (NREL), 3. Department of Homeland Security (DHS), 4. Federal Energy Regulatory Commission (FERC), 5. North American Electric Reliability Corporation (NERC), 6. Internet Engineering Task Force (IETF), 7. Institute of Electrical and Electronics Engineers (IEEE), 8. International Standards Organization (ISO) / IEC JTC 1/SC 41, 9. Internet of Things Consortium (IoTC), 10. Industrial Internet Consortium (IIC), 11. Open Connectivity Foundation (OCF), 12. 3rd Generation Partnership Project (3GPP), Mobile Telephany, 5G, etc. |
| A lot of research in this area, this is one example that has gained traction in the o&g sector https://www.sri.com/work/projects/internet-things-iot-security-and-privacy-center |
| IEEE 2030.5 |
| <https://www.nist.gov/topics/internet-things-iot> |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| 1. Numerous preexisting IoT devices have accumulated on energy industry networks over the years. Basic security and asset management hygiene must be invested in as well as foundational processes and expertise. Reference the DHS CDM program, for example, about requirements for full lifecycle asset management. <https://www.dhs.gov/cisa/cdm>, 2. IoT elements exist as part of a larger system that includes business processes, software, information flows, etc. This system-level aggregate view must be understood as well as the interrelationships with other systems in the operating environment., 3. Establishing such a connected view is essential for managing complexity, limiting risk, and making progress. 4. We recommend consideration of the IoT Security Maturity Model from the Industrial Internet Consortium (IIC): <https://azure.microsoft.com/en-us/blog/presenting-the-new-iic-security-maturity-model-for-iot/> 5. Cybersecurity threats for IoT infrastructure are real and must be addressed, and the modernization benefits of applying secure and standardized IoT needs further exploration and investment. Distributed Energy, Renewables, and Energy Storage is an ideal environment to vet this next generation of cyber-enabled energy technologies. |
| NAESB has dealt historically with the "administrative" aspects of the energy chain. Extending to SCADA would be a reach. |
| **Q3. For the 5G implementation, please provide your thoughts on the following:** |
| **Are there any use cases / business cases associated with the implementation of 5G that should be considered?** |
| 5G mm band frequencies will enable higher throughput connections in dense environments, but it likely doesn’t change much as compared to 4G since most use cases for us are in rural areas, or are low bandwidth. |
| Not currently applicable |
| hard to see |
| Defining the role of 5G in the transaction infrastructure - should there be a required backup? what data privacy protections should be in place? What carrier requirements are necessary regarding uptime, stability and protection? |
| 5G mm band frequencies will enable higher throughput connections in dense environments, but it likely doesn’t change much as compared to 4G since most use cases for us are in rural areas, or are low bandwidth. |
| Not from a strict 5G perspective. |
| **What are the benefits of adopting technology that supports 5G implementation?** |
| It will be more future proof. |
| increased speed, visibility |
| Facilitates faster decisions, more accurate transactions with the ability to move real-time field data rapidly |
| It will be more future proof. |
| Faster network speeds on mobile devices to allow for more data on mobile networks. |
| **What are the costs/issues/concerns associated with the adoption of the technology?** |
| Most 5G promises being made are centered around the mm band frequencies, but these frequencies are only good for very short range.  They also don’t deal with obstructions very well. |
| reliability (limited range, weather effects) |
| Availability and stability of 5G networks |
| Most 5G promises being made are centered around the mm band frequencies, but these frequencies are only good for very short range.  They also don’t deal with obstructions very well. |
| **Are there other standards development efforts that the committee should monitor?** |
| No |
| We are focused on the national security and data privacy aspects, under recent review by the Senate Judiciary Committee |
| No |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| I think 5G will be an incomplete, localized communication technology for the next several years, and as such will be of limited usefulness to NAESB or the broad energy industry |
| It might be better to have a section on mobility rather than just 5G technologies in order to cover all aspects of mobile applications. There could be a need at some point for standards modifications to specifically allow for better mobile device interaction with pipeline EBBs. |
| **Q4. For the improved data analytics, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define [improved] data analytics resulting from the digitalization of the energy industry?** |
| Data is treated as an agency asset and is managed and valued as a resource. Data acquisition, exploration and analysis is guided by TVA’s business unit goals and outcomes. Analytics helps to develop valuable insights from the data and enables data-driven decision making.  TVA is currently advancing standard methods to identify and prioritize business problems to be solved with analytics. Improving our analytical strategy would be speaking towards maximizing our production, optimizing our costs, and managing our risk.  All analytics initiatives are fueled by those areas. |
| The definition of digital technology that we use is as it applies to tools for data analytics |
| Ability to manage, selectively process, and visualize actionable data; ability to determine correlations between data sets |
| Data analytics is facilitating faster decisions, transactions, and visibility (particularly by the executive suite) into operational details. |
| Data analysis is implemented for two purposes, descriptive and predictive reporting to aid in several business functions ranging from risk management to market performance and operational insights |
| Using new tools and technology to assist in the analysis of ever increasing quantities of information. From our perspective this is really a back-office application where one might use AI and Machine Learning technologies to provide faster, more accurate analysis of the information available |
| **Are there any use cases / business cases associated with [improved] digital data analytics that should be considered?** |
| The Data & Analytics team has worked with BU’s to identify 70+ data use-cases and 180+ analytics use-cases. Uses-cases have been prioritized and the following analytics have been identified for TVA to begin to address in our Analytics Strategic Roadmap: Transmission Asset Analytics, Generation Asset Analytics, Supply Chain Analytics, Power Billing Analytics, and Business Intelligence analytics (Automation and Reporting). Other quick win use-cases are being developed in other areas as they arise. |
| Pipeline flow dynamics; time/price trading strategies; nat gas storage optimization |
| Data in transit and storage is a critical part of data analytics. Security of these functions is paramount, and not always easy given the existing network architectures. |
| Financial risk management and operational risk management |
| Enabled by lower costs of cloud data storage and processing functionality. |
| **What are the benefits of [improved] digital data analytics?** |
| Improved productivity, increased accuracy, efficient operations, economic benefits, customer insights, competitive advantage, innovation. |
| Better analytics could be used to better predict grid reliability/predictability, generally speaking. Improved insight into the energy industry generally is another potential benefit. |
| Asset optimization, improved trade performance |
| Huge increase in visibility, awareness, better and faster decision making. |
| Improved operational efficiencies and better insights into financial risks. |
| More useful information on a timely basis. Better predictive models. |
| **What are the costs/issues/concerns associated with [improved] digital data analytics?** |
| Costs for storage/usage of data can be costly for high volume, high frequency data; lack of resources to develop advanced analytical models, lack of skillsets and knowledge of advanced modeling techniques. |
| There are inherent costs associated with improved digital data analytics, such as costs related to hardware, storage/CPU/computing infrastructure, compliance, data retention, reliability, personnel, and implementation. |
| Shortages of: 1) platforms able to handle large data 2) personnel with applicable experience |
| Various technologies adopted before testing and validation. Often companies end up with a solution not-so-fit-for-purpose after considerable expense. |
| Failure to implement useful data analytics can lead to blind spots that can have severe business consequences (i.e. GreenHat default) or a failed opportunity to improve business performance |
| **Are there other standards development efforts that the committee should monitor?** |
| Standards and usage guardrails for analytics tools don’t exist yet at TVA. Users have to find their own way to a tool, and are at risk of picking the tool that does not adequately meet their usage needs. Our Technology Stack Team is in the process of developing standards and rationalization around analytics tools which will help users with their technology decisions. |
| Should be considered with IOT data |
| DHS did several large studies into best practices but no standards resulted. |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| The dream of every data driven organization is to be the disrupter in the industry, and to not be disrupted by the industry.  Applying the correct analytics to the right initiatives at the right time with the right people helps us get closer to being able to achieve this. |
| There should be general standards or expectations with regards to machine readability and transparency as the industry relies on improved digital data analytics. Also note that many analytical techniques leverage open-source software and big data. |
| Many data analytic solutions will be proprietary - how can NAESB's standardization efforts best benefit/enhance data analytics? |
| The various methods used in descriptive and predictive analytics, i.e. Machine learning algorithms, deep learning methods and other statistical methods, i.e. Random Forests that may be worth developing a standard model for the industry |
| **Q5. For renewable energy certificate tracking/accounting, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define the tracking/accounting of digital renewable energy certificates?** |
| Internally we use a combination of spreadsheets and third-party software to manage our portfolio of RECs.  Additionally, a portion of the portfolio of RECs is subject to the certification requirements for Green-e and NAR tracking |
| Not currently applicable |
| Not my area |
| Reliance on purely digital systems to produce, store, track, and transmit RECs in a secure fashion |
| Not involved with Renewable Energy Certificates. |
| **Are there any use cases / business cases associated with [improved] digital renewable energy certificate tracking/accounting that should be considered?** |
| All of our REC portfolio management functions are currently executed via digital tracking accounting. |
| Data integrity, storage and handling standardization would be very beneficial |
| **What are the benefits of digital renewable energy certificate tracking/accounting?** |
| Digital REC tracking accounting is the most efficient way to track and report on the REC position, as well as providing a clear look into the portfolio activity for audit purposes. |
| An area ripe for standardization. |
| **What are the costs/issues/concerns associated with digital renewable energy certificate tracking/accounting?** |
| There are costs associated with the software used to manage the portfolio, which must be managed.  Depending on the vendor / software – there may be concerns about the quality of data and the reliability of the application. |
| In my world, what an adversary could do with the info, or do to change the info is important, and not well-studied. |
| **Are there other standards development efforts that the committee should monitor?** |
| REC contract standardization will better enable renewable DER as it evolves. |
| None at this time |
| NREL did a significant study in this space several years ago, but no standards resulted |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| None at this time |
| I am not very familiar with Energy Certificates. Could this be a good application for using digital ledger technology to trade Energy Certificates like they do with bitcoin? |
| **Q6. For distributed energy resource communication protocols, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define distributed energy resource communication protocols?** |
| We define them as applications used to manager DER systems on the distribution grid (i.e. Local Power Company managed). |
| Not currently applicable |
| Not my area |
| We consider this part of all comm protocols, but in the operational environment, the value of the data in transit is higher, in a higher consequence space. |
| IEEE 1547-2018 and IEEE 2030.5 are key building blocks |
| **Are there any use cases / business cases associated with distributed energy resource communication protocols that should be considered?** |
| One of the main business cases is to control DER systems as needed to support grid reliability and safety. Another is to track, manage, and report performance. |
| In the operational environment, more obscure protocols have remained valid due to their inherent 'security through obscurity'. Understanding the risks with standard vs non-standard protocols would be useful. |
| California PUC RESOLUTION E-5000 July 11, 2019 |
| Not involved with Distributed Energy Resources. |
| **What are the benefits of digital distributed energy resource communication protocols?** |
| You can have an awareness of DER systems and accessibility to control them as needed to support your grid reliability. |
| A consensus on a valid protocol (benefits, risks, ROI, etc.) would be very helpful. |
| More precise command and control and situational awareness for grid operators |
| **What are the costs/issues/concerns associated with digital distributed energy resource communication protocols?** |
| TVA does not manage the distribution grid, and as such the communication protocols will have to be implemented by individual LPCs across the TN Valley. There is a risk of not adoption a standardized and consistent communication protocol across the TN valley. |
| Varying protocols menas there is no standard target, but also slows down the ability to transact across varying systems, legacy systems, etc. |
| **Are there other standards development efforts that the committee should monitor?** |
| None at this time |
| IEEE 2030.5 |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| None at this time |
| Implementations of IEEE 1547-2018 in Hawaii and California, along with CA Resolution E-5000 |
| **Q7. For use of deployable shareware, please provide your thoughts on the following**: |
| **How should the energy industry, or how does your company, define its use of deployable shareware?** |
| Not currently applicable, unless open source software is considered deployable shareware. |
| Unclear what this is... |
| Shareware can have a lot of pros & cons. The benefit to using it for transactions would need to be clearly identified. |
| Should we consider using something like “Open Source Business Applications” here rather than “Deployable Shareware?” Traditionally, anything associated with “Shareware” has been avoided in most organizations. However, we are beginning to talk more about back-office usage of some of the open source databases and business applications in the cloud. |
| **Are there any use cases / business cases associated with deployable shareware that should be considered?** |
| No responses provided |
| **What are the benefits of deployable shareware?** |
| No responses provided |
| **What are the costs/issues/concerns associated with use of digital deployable shareware?** |
| The open-source nature of the software could leave it more vulnerable to cyber attacks? |
| **Are there other standards development efforts that the committee should monitor?** |
| No responses provided |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| I still don't have my mind totally wrapped around this concept for our use cases. I'm working on it. |
| **Q8. Regarding cybersecurity, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, ensure the cybersecurity of its digital technologies?** |
| TVA reviews technology before connecting with systems or data. We perform reviews of security controls, contract language, industry threat/privacy assessments, and third party certifications to ensure the protection of TVA systems and data. The industry could serve each other in the sharing of assessments and provide vendor pressure for applying cybersecurity principals and guidance for industry technologies. |
| General cybersecurity and information security measures can include policies and procedures, training, monitoring, and following general best practices regarding protecting password security, encryption, keeping software updated, and general business continuity and disaster recovery practices. |
| We should (and do) maintain minimum industry security standards and continually revise and enhance them. |
| Ensure integrity, stability, confidentiality, and availability of all data and processing capability in energy transactions. |
| NERC CIP Standards and FERC Order 850 are key to protecting the Bulk Electric System from cyber attacks |
| Adherence to governmental guidelines. The pipeline industry is working with DOE to enhance cybersecurity measures. Our CyberSecurity and SCADA Network teams work closely with DHS (dept of homeland security) and are also evaluating common practices at the ICS (industrial control systems) CyberSecurity level. |
| **Are there any use cases / business cases for the cybersecurity of digital technologies that should be considered?** |
| Use cases should always be considered based on the risk associated with the device and data. For example, a “sensor only” device should be followed by human validation before proceeding with an operational change. A “sensor only” device can also be considered a consumable based on cost and function. |
| Protections with regards to proprietary data should be part of what is considered. |
| This is endless, but key elements for NAESB should be any data communication-related scenarios. |
| Permeates across all our topics. It needs to be addressed as an integral part of the transaction - just like safety of an operational environment. |
| Verification of Software objects prior to installation within any grid operators (transmission, distribution and generation levels) command and control systems |
| **What are the costs/issues/concerns associated with the cybersecurity of digital technologies?** |
| TVA has cost associated implementing and testing proper controls of digital technologies. This includes monitoring of controls to insure the confidentiality, integrity, and availability of the data. Additionally, some controls can yield process change and/or training personnel. We have also seen cost reduction and elimination of errors with automation. |
| There are inherent costs associated with general cybersecurity and information security include training, software costs, costs associated with breaches and reporting, and costs of updates, compliance, personnel, etc. |
| Again endless, but the key costs are the cost of constant enhancement/revision and the real costs of a breach. |
| Again, a lot of technology fielded without appropriate testing or applicability. This introduces considerable risk. |
| Becoming more challenging as more DER's come online with their embedded software code |
| **Are there other standards development efforts that the committee should monitor?** |
| The Cybersecurity industry provides multiple development efforts from government (e.g. NIST), professional trade (e.g. Center for Internet Security), and standards (e.g. IEEE). These should be regularly reviewed for reasonable expectations with vendors and industry members. |
| The NIST standards are a helpful guideline/best practice to follow, as they apply to the energy industry. |
| A ton of best practices, guidelines, and federal recommendations out there, aligned mostly per sub-sector. |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| There should not be a proscriptive requirement in most cases as it is not a one size fits all industry, but industry best practices or standards would be helpful and would help justify the cybersecurity and information security protections and costs associated with establishing such protections. It also would help to have a more centralized location for industry specific best practices. Piecemeal requirements make compliance more difficult. |
| While difficult, NAESB could be a position to act as a repository or clearing house for sharing cybersecurity tips, notices or info across the energy industry. |
| Even with best practices, we still see significant events like the EDI event last year. Incentivizing security is key, certainly standards from an industry group such as NAESB provide a huge value. |
| **Q9. Regarding digital applications of energy usage data, please provide your thoughts on the following:** |
| **Are there any use cases / business cases associated with the digital applications of energy usage data that should be considered?** |
| Not currently applicable |
| Energy resource planning, retail energy usage/offerings, energy conservation |
| Again, back to integrity of the data in storage and transit, as well as assigning a value/criticality to the data. Without this value, it is tough to ensure the right protections and handling exists within the technology. |
| Not that I am aware of from the WGQ perspective. This item appears to be geared towards retail markets where monitoring real-time energy usage information would help with demand management and prediction. |
| **What are the benefits of digital applications of energy usage data?** |
| Reduced energy costs, energy conservation, more profitable energy purchasing/trading |
| Facilitates faster, more accurate decisions. Also feeds into operational models which add to stability, uptime, and trending analysis. |
| **What are the costs/issues/concerns associated with the digital applications of energy usage data?** |
| Privacy, varied localized regulatory schemes |
| Many new to the industry do not understand data ownership and chain of custody. |
| **Are there other standards development efforts that the committee should monitor?** |
| Greenbutton |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| NAESB can provide standardized data formats that can serve as the basis for energy data storage/transfer/analysis |
| **Q10. Regarding data governance, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define data governance related to digital technologies?** |
| Data Governance helps us to define a uniformed approach in becoming a data driven organization.  It breaks down silos while encouraging collaboration which ultimately allows us to focus on the customer and to be able to extract the most amount of value we can from our data. |
| General data governance protections include performing backups, retention, destruction, distribution, privacy, and access controls. |
| Application of regulatory and ethical rules regarding the collection, transmission, storage and use of data, especially customer data |
| This is a huge issue that crosses all the data topics, if not all of the topics. As the representative body for energy transactions, NAESB membership should definitely have a voice in future data governance. |
| A well defined and adhered to data governance program can avoid many misunderstands in data usage that could have severe consequences |
| Overall management, validation and security of data within an organization. Again, this is a back-office function for our company managed at the corporate level. |
| **Are there any use cases / business cases associated with data governance related to digital technologies that should be considered?** |
| There are many.  Use cases range from data lake management, enabling the agency to search and shop for data, reducing the report stack by vetting / certifying those that are published, data quality mechanisms, master data management practice, and many more. |
| Protections with regards to proprietary data and such data needs to be available when needed and easily retrievable. |
| For NAESB, any data standardization or communication activity can be considered |
| Again, data handling including governance for data ownership, storage, protections, and transmission would be very useful. |
| ISO New England has had a data governance program in place since 2012 |
| Perhaps with some of the Cloud hosting companies like Amazon and Google. |
| **What are the costs/issues/concerns associated with data governance related to digital technologies?** |
| The cost of good data governance is multi-faceted. There are the technology costs of Metadata Management, Data Quality, and Master Data Management tools.  Then there is also the more cultural / labor intensive costs that come from having the business units understand the value governance brings and what our analytics vision is. It takes deliberate allocation of time and resources from the business working with the data governance core team to extract the most value we can from our governance initiatives. |
| Data governance shares some of the same computing infrastructure required to perform data analytics. There are some additional software costs associated with data governance of digital technologies, such as backup software or software to replicate. |
| Walking the thin line between practice and policy |
| Without clear governance, significant risk can occur, divulging data or risking integrity of the data used to make operational decisions. Without standards, mishandling and negligence can be a murky subject. |
| **Are there other standards development efforts that the committee should monitor?** |
| Engagement, Data Quality, Data Landscape Assessments, Proliferation of Reporting, just to name a few. |
| FIPS and NIST have general guidelines under development with regards to information systems and security controls, etc. |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| Being a data driven organization means being purposeful and deliberate with what we do with our data.  Data Governance helps us get there. |
| The energy industry would benefit from some best practices or general guidances for data governance of digital technologies. |
| The non-policy parts of this are NAESB's domain. The trick is to make useful, timely standards. |
| Look for best practices throughout industries |
| **Q11. Regarding cloud hosting, processing, transit and storage, please provide your thoughts on the following:** |
| **How should the energy industry, or how does your company, define/manage its interaction with the “cloud?”** |
| TVA defines the cloud as any software, platform or infrastructure that is provided by an outside entity. |
| Cloud procurement is a private contracting matter. |
| Cloud is now an integral part of processing and storing 'big data'. In many cases, processing and handling data would not be technically feasible without the cloud. |
| As an organization, we have embraced cloud technology in terms of data storage and governance, and are exploring many of the other cloud services being offered such as analytics with Machine Learning and Artificial Intelligence. |
| **Are there any use cases / business cases associated with the “cloud” that should be considered?** |
| With the rising costs of on premise storage, companies could deliver a quick win by implementing storage spaces with larger providers. This is especially true with archival data that needs to be kept for compliance but is not accessed on a regular basis.  Companies that host their own solutions or offer an “on-prem” version can be leveraged for quick turnarounds. These type of solutions need to be thoroughly vetted though. |
| 1. Businesses can be run entirely on the cloud including data analytics and cybersecurity on the cloud. 2. Businesses can share files, distribution, and expedite computing activity in the cloud. |
| Cloud security is not transparent in many cases. Heavy reliance on the supply-chain. If baseline security standards existed, companies could use this guidance to ensure the cloud meets a minimum level of security. Many times industry owners are not sure what questions to ask or where to begin, and they have to trust the provider. |
| Cloud Providers can deliver the enabling technologies for Digital Ledger and IoT implementations. |
| **What are the costs/issues/concerns associated with the “cloud?”** |
| From a cost perspective, it is important to understand that as you transition, both your on-premise and cloud solution need to run at the same time. This is the larger up front cost that is usually not factored in. Once that transition is complete, the cost will began to level out and general goes down. All cloud products are subscription-based. This means that there are ongoing costs that need to be accounted for.     Data stored in the cloud needs to be properly secured, preferably with MFA, to prevent data breaches, ransomware and lost revenue and/or reputation.  Monitoring of systems for availability and security is much different than on-premise solutions. Figuring these systems out on the front side of an effort will save time and money in the long run. |
| 1. There are capital costs and service costs and due diligence costs associated with cloud technology |
| The usual - security, reliability |
| Availability is perhaps the biggest concern currently. High availability and fault tolerance comes with a premium cost. |
| **Are there other standards development efforts that the committee should monitor?** |
| AI and ML are becoming increasingly popular and should be monitored. There is the possibility of data manipulation which would affect the desired outcome of AI/ML application. |
| **Please provide comments specific to this area that you would like the committee to consider as the report is drafted.** |
| NAESB should focus on data-centric standards (format, content, communication). How the data is stored is almost immaterial. |
| The cloud is providing companies with low cost storage and backup while offering computing power that most companies did not have available on in-house servers. This is opening a new realm of data analytics that should enhance prediction models and overall information availability. |
| **Q12: For other areas that should be examined and included in the report, but are not included in the 11 areas already identified:** |
| **Please identify others areas related to digitalization or digital technology that we should include, that could impact NAESB standards development activities.** |
| One area to consider is general standards or expectations with regards to machine readability and transparency as the industry relies on improved digital data analytics. |
| Perhaps some other mobile technologies. |
| **For each of the areas identified above, please provide information regarding (i) any descriptions or definitions you would want discussed for possible inclusion in the report, (ii) any related business cases or use cases you are aware of, (iii) any costs/issues/concerns associations with implementation, (iv) other areas of standards development to be monitored, and (v) any specific comments.** |
| (iii) Issues and Concerns around either mobile applications or web browsers deal with accessibility on both IOS and Android platforms, and with scalability for varying screen sizes of mobile devices. |
| **For each of the areas identified above, please note whether the area fits best as (i) enabling digitalization or digital technology and related services; (ii) impacted by digitalization or digital technology and related services; or (iii) impacting digitalization or digital technology and related services.** |
| The mapping that you have created to these areas is solid. I could see some potential areas of overlap in the broader topics. |
| (i) This category would be most appropriate. |
| **Q13. Please provide any additional comments:** |
| **Open-Ended Response** |
| It would be helpful to have definitions of the terms within the survey to address ambiguity about the use of such terms in the questions posed in this survey and provide a baseline understanding of such terms. |
| I can see how some of these topics could be combined, or we could have "umbrella" topics such as data governance and cyber security. The challenge in doing this is make certain the individual standards activities remain focused enough to provide valuable technical metrics and also get sizable participation from the NAESB members. In that same sense, I could also see how a standards activity may fall into more than one category. I'm curious to see if definitions in these areas are consistent among the members and if some detailed sub-topics develop into a natural prioritization. |
| Most relevant areas for NAESB to involve itself are:  Distributed Energy Resource Communication Protocols, Energy Usage Data, and Data Governance: We are early in the de-centralization of the network and when you graft Blockchain into all this, these three areas are going to be the Wild West. Getting inside before proprietary systems are built could be tricky but important in saving everyone a lot of time and $$ later on.  Deployable Shareware, Cybersecurity, and Cloud Hosting, Processing, Transit and Storage aren’t exactly related but I think of them together in this regard. They cross many other industries, and we have to be smart on what’s being done with them, but I don’t see an evident role of NAESB in standards setting.  Rec Certificates are kind of old news, and I think someone else is doing that, but its importance will only grow.  I’d like to hear if the others think we have anything to add here.  IoT and 5G are huge issues across many industries.  We’ll want to stay smart on these two but in the “crawl before you run” paradigm, I would suggest our role on an sort of standards there might not be imminent at all. |
| **Q14. Respondents:** |
| Dick Brooks |
| Valerie Crockett |
| Steven McCord |
| Annie McIntyre |
| Joelle Ogg |
| Leigh Spangler |
| Pat Wood |

**Questions for the Survey**

1. Please select all areas associated with the digitalization and/or digital technology that you are: (1) in the process of implementing, (2) are considering implementing or (3) consider important to be included in the report:

Areas Enabled by Digitalization or Digital Technology

* 1. Distributed Ledger Technology
     1. How should the energy industry, or how does your company, define Distributed Ledger Technology?
     2. Are there any (additional) use cases / business cases for the technology that should be considered?
     3. What are the benefits of adopting the technology?
     4. What are the costs/issues/concerns associated with the adoption of the technology?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  2. Internet of Things
     1. How should the energy industry, or how does your company, define the Internet of Things?
     2. Are there any use cases / business cases for technology associated with the Internet of Things that should be considered?
     3. What are the benefits of adopting technology that supports the Internet of Things?
     4. What are the costs/issues/concerns associated with the adoption of the technology?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  3. 5G Implementation
     1. Are there any use cases / business cases associated with the implementation of 5G that should be considered?
     2. What are the benefits of adopting technology that supports 5G implementation?
     3. What are the costs/issues/concerns associated with the adoption of the technology?
     4. Are there other standards development efforts that the committee should monitor?
     5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  4. [Improved] Data Analytics
     1. How should the energy industry, or how does your company, define [improved] data analytics resulting from the digitalization of the energy industry?
     2. Are there any use cases / business cases associated with [improved] digital data analytics that should be considered?
     3. What are the benefits of [improved] digital data analytics?
     4. What are the costs/issues/concerns associated with [improved] digital data analytics?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.

Areas Impacted by Digitalization or Digital Technology

* 1. Renewable Energy Certificate Tracking/Accounting
     1. How should the energy industry, or how does your company, define the tracking/accounting of Renewable Energy Certificates
     2. Are there any (additional) use cases / business cases associated with digital Renewable Energy Certificate tracking/accounting that should be considered?
     3. What are the benefits of digital Renewable Energy Certificate tracking/accounting?
     4. What are the costs/issues/concerns associated with digital Renewable Energy Certificate tracking/accounting?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  2. Distributed Energy Resource Communication Protocols
     1. How should the energy industry, or how does your company, define digital Distributed Energy Resource communication protocols?
     2. Are there any use cases / business cases associated with digital Distributed Energy Resource communication protocols that should be considered?
     3. What are the benefits of digital Distributed Energy Resource communication protocols?
     4. What are the costs/issues/concerns associated with digital Distributed Energy Resource communication protocols?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  3. Deployable Shareware
     1. How should the energy industry, or how does your company, define its use of deployable shareware?
     2. Are there any use cases / business cases associated with deployable shareware that should be considered?
     3. What are the benefits of deployable shareware?
     4. What are the costs/issues/concerns associated with digital deployable shareware?
     5. Are there other standards development efforts that the committee should monitor?
     6. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.

Areas that impact Digitalization or Digital Technology

* 1. Cybersecurity
     1. How should the energy industry, or how does your company, ensure the cybersecurity of its digital technologies?
     2. Are there any use cases / business cases for the cybersecurity of digital technologies that should be considered?
     3. What are the costs/issues/concerns associated with the cybersecurity of digital technologies?
     4. Are there other standards development efforts that the committee should monitor?
     5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  2. Energy Usage Data
     1. Are there any use cases / business cases associated with digital applications of energy usage data that should be considered?
     2. What are the benefits of digital applications of energy usage data?
     3. What are the costs/issues/concerns associated with digital applications of energy usage data?
     4. Are there other standards development efforts that the committee should monitor?
     5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  3. Data Governance
     1. How should the energy industry, or how does your company, define data governance related to digital technologies?
     2. Are there any use cases / business cases associated with data governance related to digital technologies that should be considered?
     3. What are the costs/issues/concerns associated with data governance related to digital technologies?
     4. Are there other standards development efforts that the committee should monitor?
     5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
  4. Cloud Hosting, Processing, Transit and Storage
     1. How should the energy industry, or how does your company, define/manage its interaction with the “cloud?”
     2. Are there any use cases / business cases associated with the “cloud” that should be considered?
     3. What are the costs/issues/concerns associated with the “cloud?”
     4. Are there other standards development efforts that the committee should monitor?
     5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.

1. Other areas of analysis not identified in the 11 areas specified:
   1. Please identify other areas related to digitalization or digital technology that we should include in our analysis, that could impact NAESB standards development activities.
   2. For each of the areas identified in question 2(a), please answer the following questions:
      1. Are there specific definitions or descriptions that you would want applied to this area?
      2. Are there any use cases / business cases associated with this area that should be considered?
      3. What are the costs/issues/concerns associated with implementation of this area?
      4. Are there other standards development efforts that the committee should monitor related to this area?
      5. Please provide comments specific to this area that you would like the committee to consider as the report is drafted.
   3. For each of the areas identified in question 2(a), please note which one of the three sections is most appropriate:
      1. Areas enabled by digitalization or digital technology and related services
      2. Areas that are impacted by digitalization or digital technology and related services
      3. Areas that impact digitalization or digital technology and related services
2. General Comments: