These comments are in response to **Document Number 2021-08482**, as referenced in the "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure", dated April 22, 2021. These comments represent the opinions of the Alliance Risk Group, LLC, and its Strategic Service Partners Iqumulus, ITEGRITI, and mnemonic (collectively "The Alliance Partners" or "TAP"). TAP is a Houston-based consortium of consulting and service firms that together address the cyber, digital transformation, Risk, and ESG needs of its clients. TAP's cyber services include 24/7 monitoring, detection, and incident response a well penetration testing, training, security architecture, and threat assessment services. TAP's digital transformation services include the development of artificial intelligence and machine learning models that enable TAP's clients to prevent sensitive data from being in the public domain and enable the predictability of future events.

The Current State of Cyber-Regulation in the US Energy Markets

- NERC, through FERC, has development and oversight responsibility for current CIP standards for grid security
- No standard/mandatory cyber requirements for the Oil and Gas markets yet, but this is where we have now seen a major attack. Oil & Gas has similar risk and infrastructure, and can benefit from 13+ years of NERC CIP implementation lessons learned
- Focus has been on cybersecurity of the systems that operate power assets whose loss would have the greatest impact on the Bulk Electric System (BES). Power assets determined to have a low impact to the BES have a small subset of cybersecurity requirements. The NERC CIP requirements do not include power distribution assets and business systems are not addressed.
- Cost of implementation should not be a consideration for mandatory requirements; however, companies are "for-profit" and cybersecurity controls beyond those that are required are assessed for relative risk and benefit

Securing Critical Infrastructure and the Energy Sector

Nine out of ten cyber-security incidents in the Energy Sector, start in IT systems. Modern Industrial Control Systems (ICS) are now highly automated with extensive dependencies between Operational Technologies (OT) and corporate Information Technologies (IT). The connections of OT to IP-based IT networks have introduced vulnerabilities and increased the attack surface dramatically.

Intelligence about critical infrastructure and its assets is a key objective for several nation state actors. In recent years, we have seen an increased willingness to perform cyberattacks to gather intelligence, and even perform sabotage with substantial impact. Such attacks can not only stop production and cause serious physical damage, but also put lives at risk.

A Brief Case Study: Norwegian Energy Market Cyber-Regulation

Norwegian energy regulators have been focused on the cyber-security of their energy markets for years. As a major producer of hydro-electric power and exploration of crude oil and natural gas, and as a member of NATO, Norway has been the target of several attempted cyber-attacks. By no means perfect, there is an overall lack of inspection and enforcement, but the regulations are clear and all focus on risk assessments. The regulation was improved greatly when expert consultants were asked to give input.

Norway's approach goes much further than US regulations currently do. Energy suppliers are segmented according to their relative size in their market. The regulations for each segment build on the requirements for the previous segment. There is a heavy focus on sensitive information (i.e. information that could be used to cause damage). There are strong restrictions on allowing remote access to an ICS or connecting an ICS to the internet. There are also requirements for ensuring the continued operation, or rapid recovery, of the supplier in case of disaster.

The Norwegian regulators require regular cyber-risk assessments with well-documented results from all energy producers. The regulation is called (translated) "The Regulation of Security and Preparedness in Energy Provision" and it requires a National Preparedness Unit that co-ordinates among all the energy providers, who are each required to have a Security Coordinator. These risk assessments are required for any potential threat to the operation, including environmental risks.

What We Propose

- The Energy Industry must have measures in place to manage risk when it comes to critical infrastructure. "Checking a box" is no longer sufficient. The risk programs must be regularly assessed and maintained with auditable assessment results
- Cyber-Risk should be managed with an integrated approach that considers the broad spectrum of corporate risk
- Government needs to fund the standardization of security regulations, which include cyber and physical controls, as part of the national infrastructure discussion
- Current requirements must be simplified, and future requirements done in the same way
- Quantitative scenario planning must be done. Look at the historical and current data as well as how you acquire future data. The needs to be a quantified set of scenarios that can be benchmarked

This may be done through two possible approaches:

i. A high-level planning approach that looks at the entire sector and looks at quantitative scenario planning:

TAP recommends the establishment of a national Quantitative Scenario Planning Partnership and Platform for the Energy Sector – e.g. in the form

of a public-private partnership and technology platform – where energy producers, processors, and distributors are encouraged (e.g. through targeted subsidies, tax incentives, and regulatory action) to participate and volunteer data (production, operational, environmental, cyber-security, etc.) in return for sector-wide benchmarking; resiliency scenario development; and resiliency scenario monitoring. The purpose of which to design, architect, and build a national system for increased Energy Sector resilience, that can be tracked by industry participants, lawmakers, and regulators. Most importantly, such a national system and platform can be used to *compute quantitative best practices and strategies* for Energy Sector resilience at the national, regional, and operational levels, going forward.

A complete future-state Quantitative Scenario Planning (QSP) methodology requires endogenous and exogenous data taxonomies - both consisting of multiple layers and policies - spanning social, technological, economic, environmental, infrastructural, as well as unstructured (e.g., social media, dark web, etc.) and alternative (e.g., personal handheld device telemetry). The proposed QSP practice encompasses hyperscale (billions of data points) neutral inferential models, that objectively inspect data quality and establish micro-feature correlations - 24/7/365 - but also the development of a multitude of predictive AI models that seek to continuously *featurize attributes of a living data model* specific to Energy Sector Resilience - 24/7/365. TAP is thus proposing a living - intrinsically resilient – solution to be powered by AI, to be managed by a QSP Committee of private and public stakeholders, under the oversight of the DOE.

The goal of a successful QSP partnership and platform should be one of enabling both private and public sector stakeholders to develop multiple knowable scenarios against which quantified impacts and actions can be anticipated and monitored for emergence, whether endogenous, exogenous, or hybrid in nature. More importantly, a successful QSP partnership and platform should enable all stakeholders to contribute unknowable scenarios (imagined) against which real world impacts can be tested and quantified, allowing emergence-monitoring and prescription of informed anticipatory action for a wider range of scenarios than historically thought possible.

TAP proposes such sweeping changes based on the DOE's and Energy Sector's critical roles in national security and public safety, but also from the perspective of the Energy Sector's impending exogenous shift towards decarbonization and ensuing cross-sector volatility contaminations to be anticipated. TAP believes a centralized Energy Sector QSP program to be historically critical for the DOE and the U.S.

ii. Go down to the tactical level and look at how to decouple the telemetry of the industry from online access:

TAP recommends that as part of an increased Energy Sector *physical* resilience; producers, processors, and distributors alike, across all sector verticals, are encouraged (e.g., through targeted subsidies, tax incentives, and regulatory action) to move Industrial Process and Control Systems off the open Internet going forward, and towards a modernized architectural paradigm of Edge Computing. TAP specifically recommends a modernized regulatory regimen that encourages and stimulates shifting Industrial Process and Control Systems to the edge of local or wide area networks in operational use, across the Energy Sector, and where innovation and implementation of mature Edge Computing architectures are not only openly encouraged but uniquely rewarded (e.g., through targeted subsidies, tax incentives, and regulatory action).

Edge Computing architectures in Industrial Process and Control Systems historically enable a higher level of physical security while enabling a higher Return-on-Assets across industries. This, as so-called regional computational nodes, and edge micro clouds can process data at or near the machine, without the need for centralized batch or stream processing of data (as historically connected to the open Internet) while maintaining computational capacity to run hyperlocal (e.g., on-chip AI) - machine learning algorithms that can optimize production output at the machine (off and away from the open Internet). Examples of practical applications of Edge Computing span fluid sensors and controls in oil refineries and pipelines, to gas leak detection systems aided by Computer Vision.

TAP sees a deep need for strengthened education around the Edge Computing paradigm across all verticals of the Energy Sector and would therefore recommend that the DOE also stimulate industry education programs specifically aimed at raising awareness around the *architectural paradigm* of Edge Computing itself, from a national security and public safety perspective.

Finally, a sector-wide conversion from outdated on-premise ICS architectures will likely prove cost prohibitive for large swaths of the private U.S. Energy Sector, which will entail increased and targeted subsidies of such conversion over time. Alliance recommends that the DOE promote a tiered and staggered, yet systematic, regulatory program seeking to stimulate various strata of the sector individually and over time, by volume, dispersion, risk, etc.

The Time to Act is Now

The World has experienced two major events in the past weeks: the Colonial Pipeline event and the JBS event. There exists the real possibility that these events may become more frequent and do far more damage in the future. The US is already in a state of strained infrastructure due to the supply chain consequences caused by the Pandemic. Should a major cyber-event occur again while we are in this position of reduced response capability, the economic and social ramifications could be catastrophic. TAP commends the DOE for reaching out for public comment on these matters. We trust that the DOE will consider our comments and know that solutions exist to make the US safer and better prepared for any future attacks.