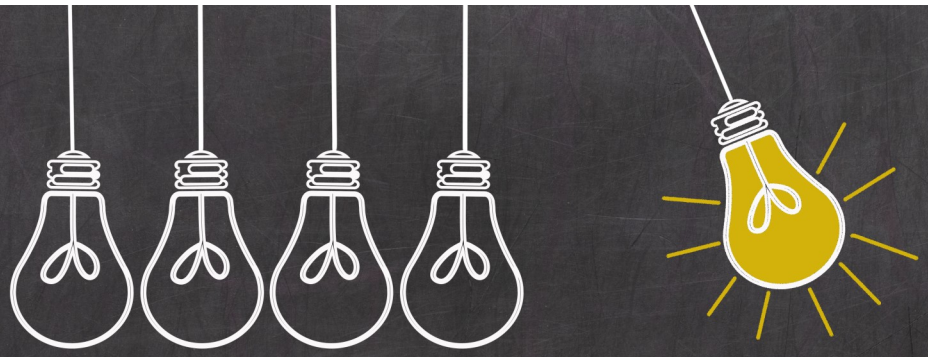
Weekly Briefing

Ellen Hughes-Cromwick



June 6, 2018

Energy Reliability and Risk Mitigation

- *A statement issued by the U.S. Administration alleges that both coal and nuclear energy sources should be subsidized in order to provide an added layer of energy security.*
- *Central to this issue is the assertion that cyber security risks pose significant danger to the electric grid, thereby supporting the view that a physical hedge is warranted.*
- *The largest natural gas pipeline companies, who have much at stake, acknowledge the risk, take it into account in their business.*

Most analysts cringe when there is mention of intervening in a market that functions fairly well. Admittedly, the conventional energy market does sit side by side to a significant negative externality, i.e., pollution. As such, the right kind of intervention — carbon tax — is a standard policy recommendation which flows from the theory of public finance. When there is an externality, fix it with a policy tool well designed to compensate for the fact that the price of this pollution is not reflected in what we pay when we consume goods which generate pollution. This reduces the externality to an "optimal" level.

Last week, the U.S. Administration ordered the Department of Energy to examine national security concerns around the "rapid depletion of a critical part of our nation's energy mix," by studying support for coal and nuclear production resources.

- This could be viewed as a simple hedging strategy. If there are critical commodities that cannot be obtained under certain risky conditions, then "physical" hedges may be justified. Physical hedges are cases where a resource is stockpiled because there is worry that flows could be disrupted, thereby causing a halt in critical economic activity and indeed, livelihood, such as we have seen in Puerto Rico with severe power disruptions.
- The Administration is pointing to cybersecurity concerns. Publicly traded energy companies have all followed the Security and Exchange Commission's guidance on identifying cybersecurity as a business risk. Industry players have embedded risk mitigation actions into their operations. Adding a layer of federal government intervention — and cost — is not economic.
- There is no question that market forces fall short of producing the most desirable outcomes for society. That is why we have, at our disposal, evidence-based policymaking. It allows for prudent adjustments to our policies in order to achieve the outcomes that we want and deserve: prosperity for all. When we veer off course and intervene in an ad hoc manner, we all lose. Spending money on coal and nuclear as the costs of renewables like solar and wind have become competitive is exacerbating what is already a sizable negative externality.

Pollution as a Negative Externality

There is broad consensus, based on theory and evidence, that pollution — including CO_2 emissions from the burning of fossil fuels — is a negative externality. This means that the social costs of the "consumption" of fossil fuels exceeds the private costs (e.g., what we pay at the gas pump).

The existence of a negative externality in consumption or production warrants an intervention by government in order to address this outcome. In the case of CO_2 emissions as a negative externality, the consensus is that a carbon tax would address this externality. Why is a tax warranted? Because then we would all make better decisions about our consumption and production when all of the costs — private plus social — are transparent and fully accounted for.

Kinder Morgan's 2017 Annual Report

The mention of cybersecurity is the 14th risk factor identified for their business operations. This is similar to other natural gas pipeline companies.

"Terrorist attacks, including cyber sabotage, or the threat of such attacks, may adversely affect our business or harm our business reputation.

The U.S. government has issued public warnings that indicate that pipelines and other infrastructure assets might be specific targets of terrorist organizations or "cyber sabotage" events. These potential targets might include our pipeline systems, terminals, processing plants or operating systems. The occurrence of a terrorist attack could cause a substantial decrease in revenues and cash flows, increased costs to respond or other financial loss, damage to our reputation, increased regulation or litigation or inaccurate information reported from our operations. There is no assurance that adequate cyber sabotage and terrorism insurance will be available at rates we believe are reasonable in the near future. These developments may subject our operations to increased risks, as well as increased costs, and, depending on their ultimate magnitude, could have a material adverse effect on our business, results of operations and financial condition or harm our business reputation."

Kinder Morgan 2017 Annual Report