

## Opening Statement

Alan Armstrong

President and CEO, Williams

FERC Technical Conference on Security Investment for Energy Infrastructure

Panel II: Incentives and Cost Recovery for Security Investments

March 28, 2019

- Good afternoon. Williams appreciates this opportunity to address the Commission, DOE and TSA senior officials to discuss the sensitive and important topic of physical and cyber security of the nation's natural gas pipeline systems. Industry and government both have a role in ensuring pipelines make the necessary investments to keep our systems secure. The investments we've made to date have served our systems well. Williams has in place a strong program that relies on effective protocols and system redundancies.
- Williams owns and operates premier energy infrastructure across the United States, including the Transco and Northwest pipelines, two interstate natural gas pipelines regulated by this Commission, with Transco being the largest volume and fastest growing interstate pipeline system in the U.S. Williams has over 33,000 miles of pipelines, and we are sharply focused on continuing to build-out and operate large-scale energy infrastructure projects. We have over 5000 U.S. employees. Our corporate headquarters are in Tulsa, Oklahoma, and we have major offices in Houston, Salt Lake City, and Pittsburgh.
- Cyber and physical security is a high priority for Williams. We recognize that our industry – not unlike many others - faces a constantly changing threat landscape and increasingly sophisticated and adaptive adversaries. Williams acknowledges that these threats not only present a risk to Williams, but also have the potential to impact national security, the environment, and public safety. To address these threats, Williams applies a strategic, risk-based approach to protect our facilities and the technologies that enable our operations. Williams' cyber and physical security programs are oriented around the TSA Pipeline Security Guidelines and the NIST Cybersecurity Framework and include effective governance, comprehensive risk-based management, and numerous programs designed to promote the security, reliability and resiliency of our operations.

Williams has physical redundancy in both our soft and hard control systems and incorporates numerous layered defenses, backups, fail-safes and manual controls to ensure that we can safely keep gas flowing even if associated computer systems, such as SCADA, become unavailable. We maintain backup control rooms and backup data rooms in geographically dispersed locations to enable quick recovery in the event of a successful cyber intrusion and conduct regular incident response exercises to improve our readiness and ensure the resiliency of our operations. The fact is that natural gas transportation systems are designed to limit points of failure and ensure a high degree of reliability. Let me provide a real-life example. We recently experienced an extended outage (~12 hours) in our Transco Houston control center due to an event arising from

building maintenance. The maintenance work triggered a fire suppression system that shut down the power to our SCADA IT equipment room and forced an unplanned outage of our Transco pipeline control center in Houston. Very quickly, we were able to respond to this outage by mobilizing local field operations personnel who monitored and manually controlled critical field locations, allowing time to switch over to our redundant IT equipment at our back-up control center in Pennsylvania. We were able to do this without disruption to Transco's customers, and with the engineered safety systems that exist on the mechanical equipment in the field, were able to execute this safely. We are not unique in this respect, as many major pipeline operators have back-up controls centers and are able to monitor and control equipment at the local field level to minimize disruptions to the gas grid.

- Williams and INGAA's other member companies take seriously the protection of critical infrastructure. The TSA's ongoing efforts to partner with and support our industry provide the flexibility and agility our industry needs to stay ahead of these constantly emerging threats. The Commission and the other federal agencies and departments, including those represented here, can continue to play an important role by publicly supporting the TSA's efforts and the ongoing investment in cyber and physical security. Understanding the strength of the systems already in place, and how they have worked when challenges have arisen, will help inform government and industry efforts.
- As for economic incentives, our view is that the Commission's 2001 Policy Statement on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies supports pipelines' investments in security and provides the flexibility necessary for pipelines to address their unique circumstances in seeking to recover those costs. Affirmation by the Commission and other federal entities that this policy remains as important today as it was in 2001 would be an appropriate step as the Commission continues to raise awareness of security issues.
- The Commission's current means by which pipelines recover these investments, which include rate trackers, limited Section 4 rate cases, and general Section 4 rate cases, continue to be appropriate means to recover those costs. In particular, trackers and limited Section 4 filings make sense because they allow companies to time those filings more closely with the incurrence of the cyber and physical security investments, thereby giving pipelines the ability to more fully recover prudently incurred costs. Williams will continue to make investments in physical and cyber security and welcomes the federal government's recognition of the importance of these investments.
- The interstate pipeline business is a very competitive business. And, just like other competitive markets, pipelines are not guaranteed to recover all of their costs. So, with or without explicit incentives, there are no guarantees for 100% cost recovery. Pipelines have to be proactive, nimble and service-oriented to retain customers and keep volume throughput high. Pipelines have to compete for customers and have to transport the volumes used to calculate their rates, or we do not recover our costs. The Commission

can be proactive as well by ensuring the opportunity for cost recovery, including allowing returns on equity that cover the cost of capital.

- Having efficient, streamlined and predictable regulatory processes is also important. The more regulatory certainty pipelines have, the better able we are to make sound investments. That is true for the Commission's rate processes as well as FERC's certificate process, which is so important for fostering sufficient energy infrastructure in this country.
- I have prepared answers to the questions you posed in the Notice of this Technical Conference, and I have those available. I am happy to engage in today's discussion and answer your questions.

## **Panel II: Incentives and Cost Recovery for Security Investments**

### ***Cost Recovery:***

1. What role do states currently play in requiring and/or facilitating energy infrastructure security investments? Do states require industry to have plans and programs to prevent and recover from cyber and physical attacks? Is industry subject to requirements to assess risk and prioritize action based on state priorities?

*States do not play a role in interstate gas pipeline energy infrastructure security investments.*

2. Are current cost recovery policies of the federal and state governments affecting the ability of owners and operators of energy infrastructure to invest in cyber and physical security for this energy infrastructure? Do federal and state policies complement or conflict with each other? Are these policies helping or hindering security investments?

*States' policies generally do not affect interstate natural gas pipelines' ability to invest in, or to recover the costs of, cyber and physical security. For example, though Williams' Transco pipeline system operates in thirteen states, it faces no industry-specific, state-imposed cyber or physical security requirements. We believe this is a good thing and that under voluntary standards, the industry is able to be nimble and responsive to cyber-security threats. Williams is unaware of any present conflicts between federal and state policies that might hinder security-related investments in the interstate natural gas pipeline industry.*

*As a member of the Interstate Natural Gas Association of America ("INGAA"), Williams conforms to INGAA's Commitments to Pipeline Security. Participation in the INGAA Commitments requires Williams and INGAA's other member companies to implement security measures and to take other actions to ensure the resilience, security, and safety of their pipelines and associated facilities.*

*To the extent there is a constraint on interstate pipelines' ability to recover the costs of*

*cyber and other security investments, it comes in the form of new prescriptive requirements which fail to account for the competitive landscape. Having a competitive market for pipeline transportation services has many advantages for the consuming public and the US economy, as pipelines must maintain competitive rates. Due to this environment, it is important for the Commission and other agencies to avoid prescriptive new requirements that impose costs which pipelines may have limited ability to recover from their customers. The most effective means by which the Commission can foster prudent security investments is to ensure clear and consistent regulatory policies, efficient processing of pipeline certificate applications, and sufficient rates of return on equity in cost-based rates.*

3. Do cost recovery policies at the state and federal level facilitate the adoption of best practices for threat mitigation at energy infrastructures? Do they allow for cost recovery for investment to address mitigation of new and emerging threats (e.g., intentional electromagnetic interference and electromagnetic pulse)?

*As noted, because of market pressures, the role of cost recovery policies in interstate pipelines' investments to mitigate new and evolving threats is not uniform across the industry, and is more limited than it may be for other regulated entities. Nevertheless, having the flexibility to seek timely recovery of security related costs is an important means by which the Commission can promote the safety and security of the interstate pipeline network. Regardless of whether all of the costs can be recovered, Williams and INGAA's other member pipelines are committed to ensuring the security of their facilities, and, to do so, utilize various federal and state resources. These principally include: (1) the TSA Pipeline Security Guidelines; (2) NIST Cybersecurity Framework; and (3) information-sharing platforms, including the Downstream Natural Gas Information Sharing and Analysis Center and the INGAA Automated Threat Information Sharing Network Pilot Program.*

4. Is FERC's September 14, 2001 Statement of Policy on Extraordinary Expenditures Necessary to Safeguard National Energy Supplies<sup>1</sup> still helpful to facilitate investment that supports physical and cyber security of energy infrastructure, or are any revisions to the Policy Statement needed to facilitate such investment?

*The Commission's 2001 Policy Statement remains useful because it represents the Commission's overarching commitment to permitting recovery of costs related to infrastructure security. A key attribute of the 2001 Policy Statement is that it permits each pipeline flexibility to structure any cost recovery proposal it may offer in the manner best suited to its customers, its markets and the nature and magnitude of the costs it seeks to recover. We believe it is useful that the Commission has not prescribed a particular type of recovery mechanism or even a specific type of filing a company must*

---

<sup>1</sup> *Extraordinary Expenditures Necessary to Safeguard National Energy Supplies*, 96 FERC ¶ 61,299 (2001) (2001 Policy Statement).

*make to present a proposal under the 2001 Policy Statement. Pursuant to the 2001 Policy Statement, the Commission has approved security cost surcharges for several jurisdictional oil pipelines, but it also has accepted and considered other cost recovery approaches. Because of the competitive market forces that all interstate natural gas pipelines face, the kind of regulatory flexibility that the 2001 Policy Statement embodies is important and valuable, and ultimately helps to facilitate ongoing investments in resilience, security, and safety. To the extent that the Commission chooses to reinforce the validity of the Policy Statement in today's security environment, Williams would welcome and support such a move.*

5. For competitive generators that do not recover their costs through retail rates, are there mechanisms under which they may recover costs for physical or cybersecurity investments other than through their market-based rates?

*Not applicable to interstate natural gas pipelines.*

6. If federal standards, guidelines, or authorities indicate that an energy facility is high-risk or critical (e.g., designation as Defense Critical Electric Infrastructure under Section 215A of the Federal Power Act), how would such designations be considered as a company prioritizes security investments? How would such a designation be considered by state regulators when reviewing cost recovery filings for measures taken above and beyond compliance with mandatory reliability standards?

*As I noted in my opening remarks, Williams applies TSA's Pipeline Security Guidelines, which provide that pipelines will identify and give priority to protecting their critical facilities. Williams determines the criticality of our facilities using a combination of criteria based on the Guidelines, potential impact to national security and public safety, and other factors specific to Williams' operations. These criticality assessments feed into our risk management program and serve as a planning and decision support tool to assist Williams' security team with identifying, evaluating and prioritizing risks and determining appropriate and effective security measures.*

7. What factors should the states be aware of when reviewing cost recovery filings for cyber and physical security investments? Can these factors be included on an industry-wide or multi-state level?

*States do not review cost recovery filings for cyber and physical security investments by interstate natural gas pipelines.*

8. Certain events could require significant unbudgeted resources to respond effectively. How should these costs be considered by federal and state authorities for cost recovery?

*The Commission in the past was responsive and flexible when pipelines have had to respond to extraordinary events, such as major hurricanes like Rita and Katrina in the*

*mid-2000s. It is critical for regulators to recognize that, when a major emergency occurs, the owners and operators of pipelines and other energy infrastructure often have to act immediately to respond to loss of communications, damaged facilities, and other consequences to prevent or minimize risks to public safety, to their employees, and to property. In those situations, cost always becomes a subordinate factor. Based on experience, Williams is confident the Commission understands this, and that it will continue to work closely with interstate pipelines and other regulated entities in all aspects of such situations, including cost recovery, as and when they arise.*

***Financial Incentives:***

9. What type of incentives would be most effective to facilitate investment in cyber and physical security? How could costs for these incentives be recovered?

*The natural gas pipeline industry, including Williams, is already working diligently to secure the nation's critical gas transmission infrastructure from cyber and physical security threats. As mentioned, the pipeline company members of INGAA, including Williams, conform to INGAA's Commitments to Pipeline Security, which enumerate specific actions that all member companies will take to identify, protect, detect, respond to, and recover from security threats targeting our systems.*

*The industry and Williams are already investing in cyber and physical security and have strong incentives to ensure that pipeline infrastructure remains resilient and secure. That said, the industry would benefit from the Commission's continued support for these types of investments and the continued flexibility to allow each pipeline to structure appropriate cost recovery proposals. It is also important that the Commission support returns on equity sufficient to ensure pipelines can attract needed capital and in recognition of the risks faced by industry. Moreover, understanding the strength of the systems already in place and how our protocols and redundant security systems are currently working to protect our pipelines, is as important as the Commission's policies for recovering these costs.*

10. How could the Commission use its authority under Section 219 of the Federal Power Act to establish incentives for improved cyber and physical security? Are there other ratemaking or accounting changes that would help incent investments in cyber and physical security?

*The Federal Power Act is not applicable to interstate natural gas pipelines.*

*Williams suggests that the Commission continue its practice of quickly responding to cost recovery filings for unplanned security related expenditures. Another option could be legislation providing for accelerated depreciation, or similar tax incentives, for investments in physical and cyber security.*

11. Are there any grants or other cost recovery mechanisms available for industry to assist with security investments at their facilities?

*Williams is not aware of any grants or other cost recovery mechanisms available for*

*interstate natural gas pipelines to assist with security investments.*

12. What changes could federal and state authorities make to current policies to better incent the adoption of best practices for cyber and physical security at energy infrastructure facilities?

*The interstate natural gas pipeline industry, and Williams in particular, is already investing in cyber and physical security to ensure pipeline infrastructure remains resilient and secure. The Commission's 2001 Policy Statement provides a flexible framework which incents the adoption of best practices by permitting each pipeline to consider its individual circumstances in structuring a proposal for cost recovery. In the competitive market faced by interstate natural gas pipelines, there is value in having federal policies which promote such individual flexibility in how a company addresses cyber and physical security and how it seeks to recover those costs. Equally important, the Commission can ensure pipeline returns on equity consider the cost of capital needed to make such investments, and it can have clear, predictable rate and certificate processes.*

13. How should state and federal authorities prioritize incentives for various security investments? How should such incentives balance the need for improved security with the rate impact on consumers?

*The security of our natural gas transmission infrastructure is a high priority for Williams, and we are vigilant about maintaining and improving our security programs. Supporting these efforts, as well as the work the Transportation Security Administration and U.S. Department of Homeland Security are doing through the National Risk Management Center, should also be a high priority for state and federal authorities. Natural gas pipelines need the continued flexibility to seek timely and complete recovery of these costs and the ability to propose individually-tailored approaches to accomplish that recovery.*