Pipeline Cybersecurity Initiative

THIS INITIATIVE LEVERAGES THE SECTOR SPECIFIC AGENCY EXPERTISE OF THE TRANSPORTATION SECURITY AGENCY (TSA) AND THE TECHNICAL CYBERSECURITY CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) TO BETTER PROTECT PIPELINES FROM EMERGING CYBERSECURITY THREATS. THIS IS A PRACTICAL APPROACH TO MITIGATING SECTOR-SPECIFIC RISKS BY USING EXISTING RESOURCES IN CONJUNCTION WITH AN OVERARCHING STRATEGIC RISK MANAGEMENT FRAMEWORK.

Collective Action

This initiative is a team effort between pipeline asset owners and operators, CISA, TSA, and the Department of Energy. By leveraging existing resources and expertise, and adding a strategic risk management overlay, we can improve security and resilience for the pipeline sector.

The Need

TSA has completed work on an assessment platform framed within CISA's Validated Architecture Design Review (VADR) and built on the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, and NIST Special Publications specific to pipeline security and Industrial Control Systems (ICS).

This tool will provide the owners and operators of pipeline infrastructure with a comprehensive evaluation and discovery process, while simultaneously focusing on the best defense strategies associated with asset owners' specific control systems network. It will include an in-depth review and evaluation of the control system's network design, configuration, interdependencies, and its applications. This, in turn, will provide TSA and CISA with significant and valuable data to develop both short-term and long-range risk analysis assessments to assist owners and operators in developing mitigation strategies to combat adversarial cyber intrusion and attack attempts.

Next Steps

Industry partner assessments are an important component of the Pipeline Cybersecurity Initiative. As such, CISA and TSA will use three different types of voluntary assessments—ranging from single and multi-day inspections to self-assessments—to help industry partners identify and mitigate potential risks to the pipeline ecosystem. CISA and TSA expect to complete a minimum of ten multi-day Tier-I assessments during 2019, and are working to complete thirty single-day Tier-II assessments during 2019. CISA and TSA are also encouraging industry partners to utilize Tier-III self-assessments to evaluate their pipeline assets. The information gathered from these assessments will further enhance long-term pipeline cybersecurity risk analysis, planning, and coordination efforts between the public and private sectors.

Additionally, CISA is establishing several internal risk analysis teams. These teams will assist industry partners' efforts to combat threats to pipeline cybersecurity by providing the risk analyses that are a critical component of risk planning and risk mitigation efforts. Through these efforts, CISA will be able to better partner with federal and industry partners to defend the Nation's pipelines from emerging cybersecurity threats.