SESSION B: PIPELINE SECURITY

MAY 7, 2019, 11:00 AM – 12:15 PM

Natural gas pipelines collaborate with the U.S. Department of Homeland Security's Transportation Security Administration ("TSA") and the U.S. Department of Transportation ("DOT") on cybersecurity risks and potential cyberattacks pursuant to DOT's 2002 Pipeline Security Information Circular and TSA's 2018 revised Pipeline Security Guidelines, adopting the National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity. These guidelines are voluntary, leading some asking Congress to enact mandatory standards given the growth in cybersecurity threats. A panel of experts will discuss the legal landscape for natural gas pipelines and how cyber threats are changing the way they do business.

Moderator: Rebecca Gagliostro, Director of Security, Reliability and Resilience INGAA

Panelists:
Paul Davis, VP for IT Cybersecurity and Telecommunications, Kinder Morgan, Inc.
Dr. Paul N. Stockton, Managing Director, Sonecon, LLC
Ron Keen, Senior Energy Advisor, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security

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.

National Risk Management Center

THE NATIONAL RISK MANAGEMENT CENTER (NRMC) IS HOUSED WITHIN THE DEPARTMENT OF HOMELAND SECURITY'S CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). THE NRMC IS A PLANNING, ANALYSIS, AND COLLABORATION CENTER WORKING TO IDENTIFY AND ADDRESS THE MOST SIGNIFICANT RISKS TO OUR NATION'S CRITICAL INFRASTRUCTURE.

The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: **Identify; Analyze; Prioritize; and Manage** the most strategic risks to our National Critical Functions — the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination.

What We Do

Since being announced at the DHS National Cybersecurity Summit, the NRMC has hit the ground running. Specifically:

- **Protecting National Critical Functions:** the NRMC has launched a far-reaching effort across all 16 critical infrastructure sectors to identify and validate a list of National Critical Functions. This allows DHS to assess critical infrastructure interdependencies and identify risk and the impact it would have on our critical functions.
- **Information and Communication Technologies (ICT) Supply Chain Risk Management Task Force:** sponsored by the NRMC, the Task Force is public-private partnership to act as the federal focal point to examine and develop consensus recommendations to identify and manage risk to the global ICT supply chain.
- **Tri-Sector Executive Working Group Risk Management Activities:** chartered with senior industry representatives from the Financial Services Sector, Communications Sector, and Electricity Sub-Sector and senior government representatives from the Departments of Homeland Security, Treasury, and Energy. Efforts have been launched to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand systemic risk.
- **Pipeline Cybersecurity Initiative:** leveraging Sector Specific Agency expertise of TSA, and technical cybersecurity capabilities of the NCCIC, this initiative will work with pipeline asset owners and operators to include an in-depth review and evaluation of the control system's network design, configuration, and interdependencies.
- **Election Security and Resilience:** working with state and local election officials, law enforcement, and the Intelligence Community, DHS has led a committed federal effort to increase information sharing with state and local partners, provide technical assistance and vulnerability assessments, strengthen communication channels, and build trust.

The NRMC is also the home within DHS for risk management initiatives surrounding Electromagnetic Pulse, Position, Navigation and Timing, and securing Unmanned Aircraft Systems.

Managing Risk

The adversaries looking to disrupt our critical infrastructure are no longer shooting from the hip to see what sticks. They are increasingly strategic and deliberate in their efforts to exploit potential Achilles Heels that could cause maximum degradation to National Critical Functions.

Our response needs to be equally strategic and prioritized. It also must recognize that risk resides at a functional level that cuts across assets, organizations, and sectors. This reality is reinforced by the cross-sector importance of supply chain risk management and technologies like Position, Navigation, and Timing.

Over the past decade, strong progress has been made to mature our mechanisms for public-private information sharing, and promote steady engagement through the National Infrastructure Protection Plan Framework and 16 sector structure. This is a solid foundation that must act as a springboard for even deeper partnership.

The NRMC looks to turn this engagement and awareness into collective action.

By understanding what is truly critical, where key dependencies and interdependencies lie, and the potential cascading impact of threats, we can identify pockets of risk we deem to be unacceptable for the nation.

Protecting National Critical Functions is a key component of the recently released National Cyber Strategy, and featured prominently in the Joint National Priorities developed in partnership with the critical infrastructure community.

Defending Today, Securing Tomorrow

The NRMC focuses on the long game of cybersecurity and infrastructure protection. In this capacity, it works with 24/7 operations centers like CISA's National Cybersecurity and Communications Integration Center (NCCIC) and the National Infrastructure Coordinating Center (NICC). By providing a strategic, long-term outlook to complement the daily "blocking and tackling" already taking place, the NRMC is filling a critical risk management gap. With existing operations centers focused on our mission to defend today, the NRMC is focused primarily on securing tomorrow.

Homeland Security

Cybersecurity and Infrastructure Security Agency
National Risk Management Center

REDUCING NATIONAL RISK

THE NATIONAL RISK MANAGEMENT CENTER

The National Risk Management Center (NRMC) supports CISA's Cyber and Infrastructure Security Mission by creating an environment where government and industry can collaborate within and across sectors to develop plans and solutions for reducing cyber and other systemic risks to national and economic security. NRMC turns analysis into action by developing risk management solutions.

NRMC Functions and Risk Management

The NRMC's evolved risk management efforts aim to build upon legacy programs which historically have focused on critical infrastructure from the perspective of assets and organizations, not systems and functions. This evolved approach will better address system-wide and cross-sector risks. Sector expertise should inform efforts, and influence our understanding of how to manage risk to National Critical Functions.

1 IDENTIFY

- **Document national critical functions**
- **Convene stakeholder groups connected by functions**
- **Identify and validate scenarios of concern**

2 ANALYZE

- **Develop Risk Register**
- **Conduct cross-sector risk assessments**
- **Improve risk analysis with shared data**

3 PRIORITIZE

- **Overlay the risk register with analysis of readiness for action to better understand gaps and opportunities**
- **Use this visibility to plan for key efforts of joint risk management activity**

4 MANAGE

- **Convene teams to develop collaborative strategies**
- **Coordinate risk management and implementation plans**

NRMC Strategic Risk Management Process

1 IDENTIFY — 2 ANALYZE — 3 PRIORITIZE — 4 MANAGE

NRMC ESTABLISHES LISTS OF NATIONAL CRITICAL FUNCTIONS (NCF) through collaboration with Sector Coordinating Councils (SCC), the Sector Specific Agencies (SSA), State, Local, Tribal, and Territorial (SLTT) partners, and other stakeholders. Sector-Specific Plans were used to identify draft NCFs to discuss with sectors such as:

- Generate Electricity
- Resilient National Positioning, Navigation, and Timing Services
- High Frequency Trading/Payments
- Treat Raw Water for Potable Use

NRMC APPLIES RISK SCENARIO ANALYSIS to understand threats, vulnerabilities, and consequences that degrade National Critical Functions.

Function	Scenario of Potential Degradation
Generate Electricity	Analysis Performed
Resilient National Positioning, Navigation, and Timing Services	Analysis Performed
High Frequency Trading/Payment	Analysis Performed
Treat Raw Water for Potable Use	Analysis Performed

Build National Risk Register that **PRIORITIZES LIKELIHOOD, CONSEQUENCE, RISK, AND READINESS.**

	Function	Likelihood	Consequence	Risks	Readiness
Tier 1	Scenario 1	(High)/Med/Low	Economic Security	(High)/Med/Low	High/Med/(Low)
Tier 1	Scenario 2	(High)/Med/Low	National Security	High/(Med)/Low	High/Med/(Low)
Tier 2	Scenario 3	High/(Med)/Low	Economic Security	High/(Med)/Low	High/(Med)/Low
Tier 2	Scenario 4	High/(Med)/Low	Public Safety	High/Med/(Low)	(High)/Med/Low

NRMC WILL LEAD COLLABORATIVE RISK MANAGEMENT EFFORTS.
Mechanisms for doing so, but not limited to:

- Establishment of Task Forces
- Integrated Planning Teams
- Studies and Analyses
- Awareness Campaigns
- Setting Research and Development Priorities

Information shared through the NCF effort will **HELP THE COUNTRY BETTER UNDERSTAND RISKS** and **IDENTIFY RISK-REDUCTION STRATEGIES FOR IMPLEMENTATION.**

Critical Infrastructure is more resilient — national and economic security, public health and safety are protected.