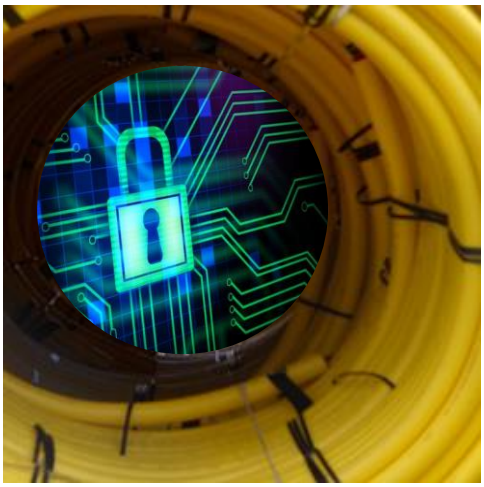
GAS TECHNOLOGY INSTITUTE

Improving Cybersecurity for Local Distribution Companies

PREVENTING, DETECTING AND MITIGATING CYBER THREATS



Working in coordination with AGA, SRI International, national laboratories, and other industry partners, GTI's initiative will focus on technology evaluation and transfer, as well as outreach and education

AGA	GTI	GTI Partners
Broad industry advocacy	Vulnerability assessment	Cylance: penetration testing
Industry strategy	Technology assessment	SRI: counter-measure development
Legislative review	Technology development	DHS: infrastructure security
Regulatory Interface	Capability improvement	EDD: graph trace analysis and modeling
Standards	Training	National Labs: technology transfer and training

For more information, contact Jim Marean
Senior Program Manager,
Energy Delivery & Utilization
312-320-9407;
james.marean@gastechnology.org

Natural gas utilities have an ongoing commitment to enhance the security of our nation's energy delivery systems, addressing both physical infrastructure and cybersecurity concerns. As part of the their leadership on cyber defense, natural gas stakeholders have identified baseline standards and practices to guide information-sharing efforts and will continue to review legislation and regulations and advocate for the industry.

A platform for sharing threat information has been established by the American Gas Association (AGA). Launched in September 2014, the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC) allows sharing of timely, relevant, and accurate cyber and physical threat intelligence, incident information, analytics, and tools. The next steps are to address the technology needs of the industry.

Gas Technology Institute (GTI) is establishing a multi-year collaborative between local distribution companies (LDCs) and the Department of Homeland Security (DHS) to address high-priority cybersecurity technology issues. A workshop hosted by GTI in April 2014 identified the highest priority areas as:

- Asset management of devices and systems capable of proving a pathway for cyber-attack and malicious activity
- Detection of a cyber-attack and/or a malicious activity

GTI will work through the collaborative to evaluate—and where appropriate—implement state-of-the-art technologies focused on the prevention, detection and mitigation of cyber threats. We have access to nearly twenty technologies developed by the national labs and vetted by DHS that are available for immediate transition to practice with LDCs.

As part of Outreach and Education efforts, there will be training for internal and contracted personnel about cybersecurity. The experience of DHS and SRI International with LOGIIC (Linking Oil and Gas Industry to Improve Cybersecurity) will be leveraged, and activities will align with AGA's Cybersecurity Strategy Task Force and their focus on broad industry advocacy and related strategies.

The cost of participation is $15,000 per utility per year. DHS is providing 50/50 matching for every dollar invested in the program up to a total of $200,000 annually.