Interstate Natural Gas Association of America (INGAA) Automated Cyber Threat Information-Sharing Network

November 2016

CHALLENGE: Apply the INGAA Automated Network to Broader Share of Energy Sector Stakeholders

Through pilot testing completed in 2015, the Interstate Natural Gas Association of America (INGAA) Automated Cyber Threat Information-Sharing Network, which uses the Confer platform, a cloud-managed, host-based cyber threat network, successfully enabled certain INGAA member organizations to exchange valuable cyber threat intelligence affecting the Energy Sector with minimal configuration and effort. However, because some INGAA member organizations have differing network and endpoint threat management solutions—some use commercially available cybersecurity software solutions while others use custom security solutions—it is uncertain whether or not the INGAA Automated Network can be used by a broader group of participants in the Energy Sector to share cyber threat information. In addition, more analysis is needed to determine how the INGAA Automated Network can be applied to industrial control systems. This project will focus on how to integrate these various security solutions across the Network while maintaining information-sharing capabilities and the collaborative community environment.

APPROACH: Research a Variety of Platforms and Develop a Network That Can Be Deployed Across a Diverse Group of Companies with Multiple Security Solutions

INGAA will research and evaluate other potential information-sharing platforms to determine which one has the best capability for allowing a diverse group of participants with multiple security solutions to exchange valuable threat intelligence with minimal configuration and effort. INGAA will evaluate the platforms for their ability to (1) operationalize large amounts of threat intelligence with little or no manual or human interaction; (2) protect privacy and safeguard shared information; and (3) be deployed and administered easily without risk to operational environments.

The goal of the project is to select a platform that will enhance the INGAA Automated Network so that participants with a variety of network security and endpoint threat management solutions can automate the sharing of intelligence. The enhanced Network will then be able to detect and defend against cyber threats earlier and to facilitate bidirectional threat sharing across a broader share of the Energy Sector.

INGAA will assess and analyze the platforms and develop a threat sharing framework that could also serve as a model for Information Sharing Analysis Centers (ISACs), the Federal government, or other private sector organizations.

NEXT STEPS: Analyze and Report on Platform Expansion and Value

- Develop metrics for vendor selection, interview potential vendors, and, upon selection, will execute a vendor contract.
- Develop user agreements and provide guidance to participating INGAA members to deploy the Network on their system(s).
- Facilitate and gather feedback through regular communications.
- Use the results of the project to develop an ongoing assessment process and report to the National Institute for Hometown Security (NIHS) at regular intervals on the conclusions and analyses.
- Success of the project can be measured by expanded use of the INGAA Automated Network by a diverse group of INGAA members, ISACs, and other Energy Sector stakeholders.

The National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge is managed by the Office of Infrastructure Protection, within the National Protection and Programs Directorate of the Department of Homeland Security (DHS), in partnership with the National Institute for Hometown Security (NIHS). To learn more about this project, contact Jay Robinson, Program Manager, DHS, at Jay.Robinson@hq.dhs.gov or Ewell Balltrip, CEO, NIHS, at eballtrip@thenihs.org.

Homeland Security