Pipeline Security

2015 RRC/PHMSA Training and Qualification Conference
Wednesday September 16, 2015
4:30 – 5:00 PM
Topics Areas for Discussion

- MOU Between TSA & PHMSA
- TSA Pipeline Security Guidelines
- National Strategy For Transportation Security
- CYBERSECURITY
MOU Between TSA & PHMSA

• In 2004 and 2006 an MOU agreed upon to delineate clear lines of authority and responsibility and promote communications, efficiency, and non-duplication of effort through cooperation and collaboration between the parties in the area of transportation security based on existing legal authorities and core competencies.

• PHMSA is responsible for administering a national program of safety in pipeline transportation including identifying pipeline safety concerns and developing uniform safety standards.

• The parties commit themselves to coordinate, to the maximum extent practicable, their programs and activities in order to improve transportation security in the United States while minimizing duplication, disruptions to transportation operations, and costs imposed on transportation stakeholders and the public.
MOU Between TSA & PHMSA

- Identification of Critical Infrastructure/Key Resources and Risk Assessments
- Strategic Planning
- Standards, Regulations, Guidelines and Directives
- Inspections and Enforcement
- PHMSA Technical Support
- Sharing Information During an Emergency Response
- Public Communication, Education and Outreach
- Communicating Protective Measures to Affected Organizations
- Legislative Matters and Budget
TSA Pipeline Security Guidelines

Topics included in Guidelines include:

• Corporate Security Program and Plan
• Risk Analysis
• Facility Criticality
• Facility Security Measures
• Cyber Security Measures
• National Terrorism Advisory System (NTAS) Threat Level Protection Measures
• Appendix A covers recommended recurring actions
NATIONAL STRATEGY FOR TRANSPORTATION SECURITY

2014 National Strategy for Transportation Security Pipeline Subsector Plan
National Strategy Security Plan

The purpose of the National Strategy for Transportation Security (NSTS) Pipeline Subsector Plan is to define national pipeline security goals, objectives and activities collaboratively developed with industry stakeholders to reduce risks posed by terrorism while enhancing the resilience of nationally significant pipeline systems. This plan builds on existing Surface Division and Pipeline capabilities and capacity, aligns with overarching, DHS, TSA, OSPIE, and Surface Division outcome-based goals, objectives, support initiatives, and activities and meets requirements of 49 U.S.C. 114(s).

Pipeline transportation risk is dominated by the risk of an improvised explosive device (IED) or vehicle-borne improvised explosive device (VBIED) attack on critical pipeline infrastructure.
National Strategy Security Plan

NSTS Goal 1: Reduce the risks and enhance resilience associated with terrorist attacks to transportation systems

- **Pipeline Strategic Objective 1:** Improve pipeline security preparedness to deter, detect, respond to and recover from terrorist attacks
- **Pipeline Strategic Objective 2:** Reduce risks associated with dangerous articles or personnel entering security sensitive areas
- **Pipeline Strategic Objective 3:** Improve physical and cyber security of nationally-significant pipeline infrastructure.
- **Pipeline Strategic Objective 4:** Improve industry involvement in the R&D prioritization process
National Strategy Security Plan

NSTS Goal 2: Enhance effective domain awareness of pipeline systems and threats

- **Pipeline Strategic Objective 1:** Improve the quality and timeliness of intelligence and information products
- **Pipeline Strategic Objective 2:** Improve public’s situational security awareness in high capacity transportation locations
- **Pipeline Strategic Objective 3:** Improve collaboration between private sector and the federal government regarding intelligence and information sharing
- **Pipeline Strategic Objective 4:** Improve situational awareness of multi-domain threats with potential to impact transportation systems
On June 26, 2015, TSA issued a message regarding a terrorist attack on a French industrial facility. An apparent terror attack occurred at a gas plant located in southeastern France, owned by Pennsylvania-based Air Products Corporation southeast of Lyon, France. A vehicle rammed the gate at the entrance to the factory and an explosion followed shortly thereafter.

At least one suspect is in custody; investigation is ongoing. The owner of the factory, Air Products, said all its employees are accounted for and have been evacuated from the site.

The French government has raised its security alert to the highest level as a result of the attack.
Security Awareness Message

- TSA recommends that operators who transport hazardous materials review their security and response plans to ensure that the plans address topics such as reporting and responding to emergencies.

- Operators are encouraged to instruct employees, contractors, and vendors to be alert and follow emergency notification procedures to immediately report to the appropriate law enforcement agency any situation that appears to constitute a threat or suspicious activity.

- TSA also recommends that operators maintain ongoing communication with federal, state, and local law enforcement agencies.
• Reference a presentation done at AGA Conference titled “Cybersecurity and the Natural Gas Industry (using the DoE ONG-C2M2)”

Level-Setting our Cybersecurity Understanding

Protecting Natural Gas Systems:

Cybersecurity

Cyber threats are real and unrelenting for all critical infrastructure. The natural gas industry must continue to employ prudent policies and practices to help ensure the resiliency and safety of natural gas systems.

Cybersecurity efforts must constantly acclimate to persistently dynamic threats. Only through an environment that fosters increased operator awareness and training, enhanced government-private cybersecurity information sharing and partnership, and flexibility to deploy appropriate strategic platforms and mechanisms can operators effectively protect, detect, mitigate, respond to and recover from cyber attacks.
• measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack – www.merriam-webster.com

• Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data.

• Cybersecurity assures protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans.

• The goal of cybersecurity is to protect data both in transit and at rest.

• Countermeasures can be put in place in order to ensure security of data.

• Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.
Cybersecurity Threats

- Protecting critical systems and information requires understanding a variety of cyber threat scenarios, risks and their potential impacts. Cyber attacks can negatively impact utility operations, disrupt energy service and even result in injuries or loss of life, as well as damage to a company’s reputation. AGA and its member companies are dedicated to protecting their systems and customers from a variety of types of cyber intrusions:

  - Coordinated Physical and Cyber Attack
  - Information Theft, Loss or Misuse
  - Breach of Critical Infrastructure
  - Dependency on Telecommunication Infrastructure
  - Employee Awareness

(AGA Threat Analysis project)
Threat Actors and their Motivations

- Hackers - notoriety
- Hacktivists - publicity
- Organized Crime - financial
- Nation States - political
- Terrorists - fear
The Early Days – up to 2011

- We have a firewall, we’re good
- The natural gas industry isn’t a sexy enough target
- Energy adversaries are focused on the electrics and oil companies
- We have mechanical fail safes for all operations components
- We only use SCADA to monitor
And then...Shamoon!
In the Summer of 2012

- Shamoon computer virus erased 30,000 workstations at Saudi Aramco and Raz Gas
  
  http://en.wikipedia.org/wiki/Shamoon
  http://www.symantec.com/connect/blogs/shamoon-attacks

- Eric Cornelius of the DHS Idaho National Lab invited to brief AGA Board of Directors

- Cybersecurity becomes AGA Board level issue

- AGA Board initiates Cybersecurity Strategy Task Force
  - Mixed group of senior leaders, functional experts, IT and gas operations
  - Assembled to address Cybersecurity for AGA
2013 – Cybersecurity Ramps up...

• As Ron Jibson started his chairmanship of AGA he identified cybersecurity as one of his primary issues

• The first meeting of the Cybersecurity Strategy Task Force was held in New Orleans in January 2013

• The Board of Directors initiated a simple six question survey of all AGA member CEO’s
  – Responses from all large member companies
  – Very few responses from smaller member companies
    • Did they get the survey?
    • Are they attentive to Cybersecurity?
    • What are they doing?
    • Is anybody out there?

• Also provided consensus industry comments on NIST Cybersecurity Framework
2014

(What are you doing with Cybersecurity?)

- AGA Discussed with Small Member Council
- AGA Considered building review tool from scratch
- AGA Decided to use new ONG-C2M2
  - Oil and Natural Gas Cybersecurity Capability Maturity Model
  - Tailored from ES-C2M2 released the previous year
- Offered facilitated C2M2 to Small Member Council companies
- Four companies identified and reviewed
What is the ONG-C2M2?

A model and evaluation method that supports ongoing evaluation and improvement of cybersecurity capabilities within the ONG subsector

Objectives

- Strengthen cybersecurity capabilities in the ONG subsector.
- Enable ONG organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities.
- Share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities.
- Enable ONG organizations to prioritize actions and investments to improve cybersecurity
Timeline

- **Project initiated to develop ES-C2M2**
- **Completed 17 pilot self-evaluations**
- **ES-C2M2 v1.0 released**
- **DOE Pilots with NG Utilities**
- **First DOE-facilitated self-evaluation at NG utility**
- **AGA Workshops**
- **C2M2 v1.1 released**
- **AGA Webinar**
- **AGA Project: Self-evaluation workshops at 4 Small NG Utilities**
Maturity Model Definition:

- An organized way to convey a path of experience, wisdom, perfection, or acculturation.
- The subject of a maturity model can be an object or things, ways of doing something, characteristics of something, practices, or processes.
### Maturity Progression Examples

**Practices are governed by policy**

**Practices are optimized**

**Practices are measured**

**Practices are managed**

**Practices are planned**

**Practices are performed but ad hoc**

**Practices are incomplete**

<table>
<thead>
<tr>
<th>Progression for Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Three-factor authentication</td>
</tr>
<tr>
<td>Two-factor authentication</td>
</tr>
<tr>
<td>Passwords change every 60 days</td>
</tr>
<tr>
<td>Strong passwords</td>
</tr>
<tr>
<td>Passwords</td>
</tr>
</tbody>
</table>
### ONG-C2M2 Model Overview

<table>
<thead>
<tr>
<th>MIL3</th>
<th>MIL2</th>
<th>MIL1</th>
<th>MIL0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(advanced)</td>
<td>(intermediate)</td>
<td>(beginning)</td>
<td></td>
</tr>
</tbody>
</table>

#### 4 Maturity Indicator Levels

- **MIL3**: Includes the most advanced practices.
- **MIL2**: Includes advanced practices.
- **MIL1**: Includes basic practices.
- **MIL0**: No practices.

#### 10 Model Domains

- **RM**: Risk Management
- **ACM**: Asset, Change, and Configuration Management
- **IAM**: Identity and Access Management
- **TVM**: Threat and Vulnerability Management
- **SA**: Situational Awareness
- **ISC**: Information Sharing and Communications
- **IR**: Event and Incident Response, Continuity of Operations
- **EDM**: Supply Chain and External Dependencies Management
- **WM**: Workforce Management
- **CPM**: Cybersecurity Program Management

#### MIL 3 practices

MIL2 & MIL3 practices are progressively more complete, advanced, and ingrained; target levels should be set for each domain based on risk tolerance and threat environment.

#### MIL 2 practices

MIL1 practices are *basic activities that any organization should perform*; these are the starting blocks.

#### MIL 1 practices

MIL1 practices are basic activities that any organization should perform; these are the starting blocks.

#### No practices

MIL0 practices are *no practices*.

#### 10 Model Domains:

Logical groupings of cyber security practices — activities that protect operations from cyber-related disruptions.
Observations from AGA Program

- The ONG-C2M2 helped each participant company better understand its cybersecurity capability maturity level
- Generally the strongest domains were Asset and Change Management and Identity and Access Management
- Generally the weakest domain was Supply Chain and External Dependencies Management
- Participating companies received a range of overall scores
- Participating companies brought a number of participants into the review to cover both information technology and gas operations
  - Lively discussions occurred surrounding many of the domain practices
Recommendations for Participants

- Close maturity level one gaps
- Evaluate maturity level two and maturity level three gaps for closure
- Institutionalize the cybersecurity program
  - Ensure cybersecurity is governed by policy
  - Ensure company leadership guides cybersecurity governance
- Supply chain management has been identified as the culprit for a number of successful cybersecurity compromises in other industries
- Prioritize separation of Information Technology networks from Operational Technology networks
- Repeat the ONG-C2M2 review
  - Review / Identify Gaps / Prioritize and Plan / Close Gaps / Repeat
Recommendations for Broader AGA Membership

• Consider using the ONG-C2M2
• Consider participating in a self-evaluation workshop or regional workshop
• Participate in information sharing activities
  – DNG-ISAC
  – ICS-CERT
  – HSIN
  – FBI Infragard
• Have at least one cleared staff person to participate in classified briefings
Review Participant
Recommendations for Broader AGA Membership

• To date, all ONG-C2M2 participants have identified that participating in the review was a valuable exercise

• All participants experienced both a validation of many cybersecurity practices and identification for areas of improvement needed for some cybersecurity practices

• The review process brings together information technology professionals and operational technology professionals in an environment to discuss and review cybersecurity

• Desire to share lessons learned
Practical ONG-C2M2 Experience
The Nuts and Bolts

- Our experience demonstrated that the ONG-C2M2 review took at minimum one full, long day to complete and more comfortably it took a day and a half to two days.

- Participants generally find that it takes interacting with a couple of the domains to eventually get into a rhythm, therefore the first two domains typically take longer.

- DoE has a Facilitator Guide available on the ONG-C2M2 web page.
Thank you for your Participation