Briefing to National Association of Regulatory Utility Commissioners

February 12, 2017
"And that's why we need a computer."
Because I’m a Government Employee

Guidance Documents

National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience

• “Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making”

National Strategy for Information Sharing and Safeguarding

Purpose and Scope

“...describe the current processes used to facilitate the flow of threat information between and among all entities involved in the critical infrastructure security and resilience mission, and provide an overview of the key threat information-sharing entities which facilitate this process.”

“...limited to threat information sharing pertaining to manmade threats, including both cyber and physical threats, to critical infrastructure.”
Approach
How Threat Information Sharing Is Done
Key Threat Information Sharing Entities

1. LOCAL AND REGIONAL Information-Sharing Hubs
2. NATIONAL Information-Sharing Hubs
3. INVESTIGATIVE Entities
4. OWNERS AND OPERATORS Operations Centers
5. PARTNERSHIPS, Alliances, and Councils
Use Case 2 – Physical Use Case: Metcalf Electric Substation Incident, Santa Barbara, CA

<table>
<thead>
<tr>
<th>Organization</th>
<th>Information is obtained</th>
<th>Information documented and safeguards added</th>
<th>Information is validated and analyzed</th>
<th>Originator shares information</th>
<th>Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start: Attack on Metcalf PG&amp;E transformers</td>
<td>PG&amp;E reroutes electric power to maintain operations</td>
<td>Increase security at all PG&amp;E sites</td>
<td>PG&amp;E produces Incident and Disturbance Report</td>
<td>PG&amp;E produces Situational Awareness Report(s)</td>
<td>PG&amp;E provides CA PSAs access to substations to conduct security surveys</td>
</tr>
</tbody>
</table>

- Open law enforcement investigation into attack
- Open terrorism investigation
- DOE conducts information and coordination call with partners
- Information shared through HSIN-CI and HSIN-Dams
- NCIRC, NERC, and Energy ISAC issue alerts to members
- PG&E shares information through multiple mechanisms and channels (ISACs, Coordinating Councils)
- PG&E provides CA PSAs access to substations to conduct security surveys

Electric Substation Security Awareness Campaign kick off with 10 city roadshow
Develop Spare Transformer Equipment Program
Sponsor training event and share lessons learned
Industry makes large investments in infrared cameras, gunshot detection, seismic recorders

Increased Resilience
Additional Case Studies

Use Case 1 - Cyber Use Case: Havex and BlackEnergy Malware

Use Case 3 - International Use Case: Westgate Mall Attack, Nairobi, Kenya

Some Observations

Role of informal networks
Balance between too much and not enough is difficult
ISAO EO is very helpful...needs to include all hazards
Challenge of classified information
Disconnect between physical and cyber security staff
Questions?

Brian Scully
Director, Strategy and Policy Programs
DHS/NPPD/Office of Infrastructure Protection
Brian.scully1@hq.dhs.gov

Find the Framework online:
https://www.dhs.gov/publication/ci-threat-info-sharing-framework
Communications Sector Information Sharing

• Information Sharing is not new to Communication Service Providers

• Information Sharing by network service providers is deep and systemic, but not fully recognized.
  • Current Efforts to Characterize and Catalogue major Venues/Opportunities for Information Sharing
  • CSRIC V – Working Group 5 Information Sharing
    • https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability

• Primary Venue for Collaboration and Information Sharing:
  • DHS National Coordinating Center / Communications Information Sharing and Analysis Center (ISAC)
  • Public/Private Coordination Point for Physical AND Cyber Events
Info-Sharing Modalities

Informal
- Phone Call
- E-mail
- Teleconference
- Professional Membership
- Working Group
- Professional Conference
- Webinar
- Technical Liaison
- Technical Seminar or Conference
- Tabletop Exercise
- Full Scale Exercise
- Automated Sharing

Formal
Notional Diagram Communications Sector Information Sharing

**Network Service Providers**

- Trusted Peers & Commercial Partners
  - Network Service Providers (NSP) Group
  - Formal/Informal Peer Organizations
  - Commercial Security Services/Third Party Partners

- ISP Internal Use
  - Internal IT Enterprise Systems
  - ISP Service Delivery Network
  - Consumers / Managed Security Customers

- Government Contracts
  - DHS/CS&C ECS/E3A Customers

- Law Enforcement
  - Federal, State & Local Law Enforcement + Organizations (FBI NCIJTF, InfraGuard)

- Sector Policy & Planning
  - Comms Sector Coordinating Council (CSCC)/Government Coordinating Council (GCC)
  - State, Local, Tribal, Territorial SCC/GCC

- DHS Coordinated Information Sharing Process
  - NCCIC/DHS Portal
  - State Fusion Centers/ISAOs/Other Sector ISACs
  - NCC Comm-ISAC

- Public/Private Partners
  - Federal/State Customers (DoD, GSA, PSAPs etc.)
  - Other Critical Infrastructure Sectors (Financial Services, Electric, IT, etc.)
  - Federal/State Partners (EOP, DHS, Governor’s Office, TAGs etc.)
  - FCC/State PUCs

**NOTE:** All information received is validated prior to action.
Information Sharing Matrix

National Svc Providers

Formal/Informal Peer Organizations

Commercial Security Services/3d Party Partners

Internal IT Enterprise Systems

ISP Service Delivery Network

Consumers/Managed Security Customers

Federal, State & Local Law Enforcement and Organizations

DHS/CS&C ECS/E3A Customers

Other Critical Infrastructure Sectors

AIS

DHS/NCCIC Portal

US-CERT/ Sector ISACs

NCC/Comm ISAC

Fed/State Partners

Email

Distro List

Teleconference

Conference/Seminar

Phone
Moving Forward – Continuous Improvement

• Information Sharing & Analysis Organizations (ISAOs)

• Network Service Provider Refinements

• Automated Indicator Sharing Initiatives

• International Collaboration