



Control System Cyber Incident Handling: A Law Enforcement Perspective

Panelists:

Scot Huntsberry, FBI
Clint Baker, RCMP
Jeff Morgan, FBI

Moderator: Mark Fabro, Lofty Perch



Control System Cyber Incident Handling: A Law Enforcement Perspective

Panelists:

Scot Huntsberry, FBI
Clint Baker, RCMP
Jeff Morgan, FBI

Moderator: Mark Fabro, Lofty Perch

Introductions



- **Scot Huntsberry, FBI**

- Supervisory Special Agent Cyber Division/Computer Intrusion



- **Clint Baker, RCMP**

- Sgt, Integrated Technological Crime Unit



- **Jeff Morgan, FBI**

- Process Control Systems Analyst, Cyber Division

FBI

- FBI's cyber mission focuses foremost on serious computer intrusions.
- Trained cyber squads at all 56 field offices and FBI Headquarters.
- Dedicated analysts focused on Process Control / SCADA (PCS) issues and USG collaboration.
- Cyber Action Teams trained in PCS issues and ready to respond.
- Outreach efforts to PCS owners / operators.



RCMP

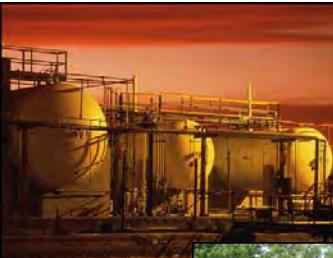
- RCMP – PS PCS Workshop 2007
- Canada's Cyber Security Strategy
- Preparation for Major Security Events
- Need cross-country research labs



Emerging Issues

- **The changing landscape**

- Trending
- Chatter
- National efforts



- **Working with the public**

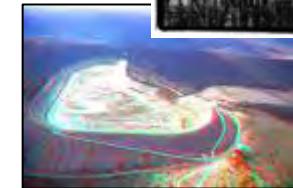
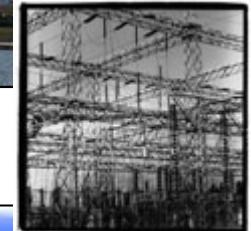
- **Working with the legal system**

- **Finding the resources/talent**



Observations From the Field

- Lessons from outreach efforts
- What investigators can/should expect
- What asset owners can expect
- Public perceptions of LE actions
- Applying current methods to SCADA/ICS



Research Initiatives – What can be done to help?

- **What is needed by L.E. to bring response capability closer to the crime**

- Incident handling
- Forensics
 - OS vendor cooperation
 - ICS vendor cooperation
- Bag and tag – how does it differ with ICS?



Open Discussion



Process Control Systems
Industry Conference