I want OT Cybersecurity:
What do I do now?

Ken Keiser
Parsons, ICS Cybersecurity, Centreville, VA
What’s not IT?

Operation Technology:
- Signaling
- Train Control / Wayside Wireless
- Access Control
- HVAC/Building Automation
- Fire/Safety
- Surveillance / IP Cameras
- Ticketing Kiosks

OT (ICS) Devices
- X5

IT Devices
OT Cyber Myths

- OT doesn’t have any cyber components
- OT systems are Air-gapped
- OT doesn’t have any Microprocessors
- No Commercial Off-the-shelf Components are in your system.
- Typical IT cybersecurity assessment techniques are safe to use on OT.
- OT Cyber problems can’t adversely effect the enterprise
- OT Operations, efficiency, and Safety are protected from IT Cybersecurity issues.
OT Cyber Myths

• OT doesn’t have any cyber components
• OT systems are Air-gapped
• OT doesn’t have any Microprocessors
• No Commercial Off-the-shelf Components are in your system.
• Typical IT cybersecurity assessment techniques are safe to use on OT.
• OT Cyber problems can’t adversely effect the enterprise
• OT Operations, efficiency, and Safety are protected from IT Cybersecurity issues.
## Difference between IT and OT

<table>
<thead>
<tr>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Availability</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity</td>
</tr>
<tr>
<td>Availability</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

- **Data is the Product**

- **Data is a tool used to make the product**

### Standards

- **NIST 800**
- **ISO 27000**
- **CCS-CSC**
- **ICS-CERT**
- **American Water Works Association**
- **WaterISAC**
## Difference between IT and OT

<table>
<thead>
<tr>
<th>IT</th>
<th>OT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confidentiality</td>
<td>• Availability • SAFETY</td>
</tr>
<tr>
<td>• Integrity</td>
<td>• Integrity • Confidentiality</td>
</tr>
<tr>
<td>• Availability</td>
<td></td>
</tr>
</tbody>
</table>

Data is the Product

Data is a tool used to make the product

Framework

- NIST 800
- ISO 27000
- ISA
- ICS-CERT
- Center for Internet Security CCS-CSC
- American Water Works Association
- WaterISAC
Don’t forget credit cards.
• You do have credit cards in your enterprise.
• PCI has their own standards (Payment Card Industry)
• What is a QSA? Qualified Security Assessor

IT, OT, and Payment Card Data shares some Zones
Elements of a good RFP

1. Project Overview
2. Organization background (optional)
3. Project Goals
4. Scope of Work and Deliverables
   1. ICS equipment
   2. Non ICS Equipment?
   3. Office IT space?
   4. Reports (on paper/PDF)
   5. Presentation in person?
5. Timeline
6. Technical requirements or limitations (included in SOW)
7. Point of Contact
8. Budget (range or exact limit)
9. Criteria for Selection
10. Format and Proposal Timeline

- Structure
- Timeline
- Budget
Benefits of a Master Service Agreement

1. Acts as a framework for multiple contracts
2. Work orders hold specific details and scope of work.
3. MSAs are useful for defining broad ICS Cybersecurity concepts
4. Future work orders can be added later as needed without going through another round of Terms & Conditions negotiations
5. Task orders can be simpler than full RFP
Benefits of a good cybersecurity specification

- Think beyond your own department (IT + OT together)
- Full Corporate Cooperation (C-Level buy-in)
- All have a role and stake in the process (Culture Change)
- Vendor/supplier understands what is in-scope and what is out-of-scope
- Goals are clear to vendor/supplier (in case of ambiguous technical spec)
- A baseline is established for future changes
- Helps to drive a shared vision of the project
- Clear timelines to get the project finished on-time
Questions?