

# **Process Control System Forum Information Sharing**

**Rita Wells**

Critical Infrastructure Assurance

May 18, 2005

# Security must be engineered

- A security program is not a product or a technology but an ongoing process
- Applying a countermeasure in reaction of an incident will never provide adequate security
- Solutions must be engineered
- The whole architecture needs to be analyzed to provide a defense in depth approach

# Many resources for best practices

- Involvement with the solution provider
- Outreach events
- National Laboratories
  - Control Systems Security Center
    - Idaho National Lab
    - Sandia National Lab
    - Pacific Northwest National Lab

# Interest Group “Call to Action”

<p>Why Sharing is Important</p>	<p>Issues and Concerns</p> <ul style="list-style-type: none"><li>Intellectual property</li><li>Competitive issues</li><li>Legal issues</li></ul>
<p>Organization Models</p> <ul style="list-style-type: none"><li>CERT/CC</li><li>ISACs</li></ul>	<p>What to share, how to share</p> <ul style="list-style-type: none"><li>Multiple levels of trusted access</li><li>Detailed vs. sanitized</li></ul>

# Sharing of information is critical to improving the systems

What you don't know can hurt you

- Two heads are better than one
- Security by obscurity is fragile
- “Ignorance is bliss, but bliss is not the same as security.”<sup>1</sup>

<sup>1</sup> Bruce Schneier, “Internet Shield: Secrecy and security, San Francisco Chronicle, March 02, 2003.

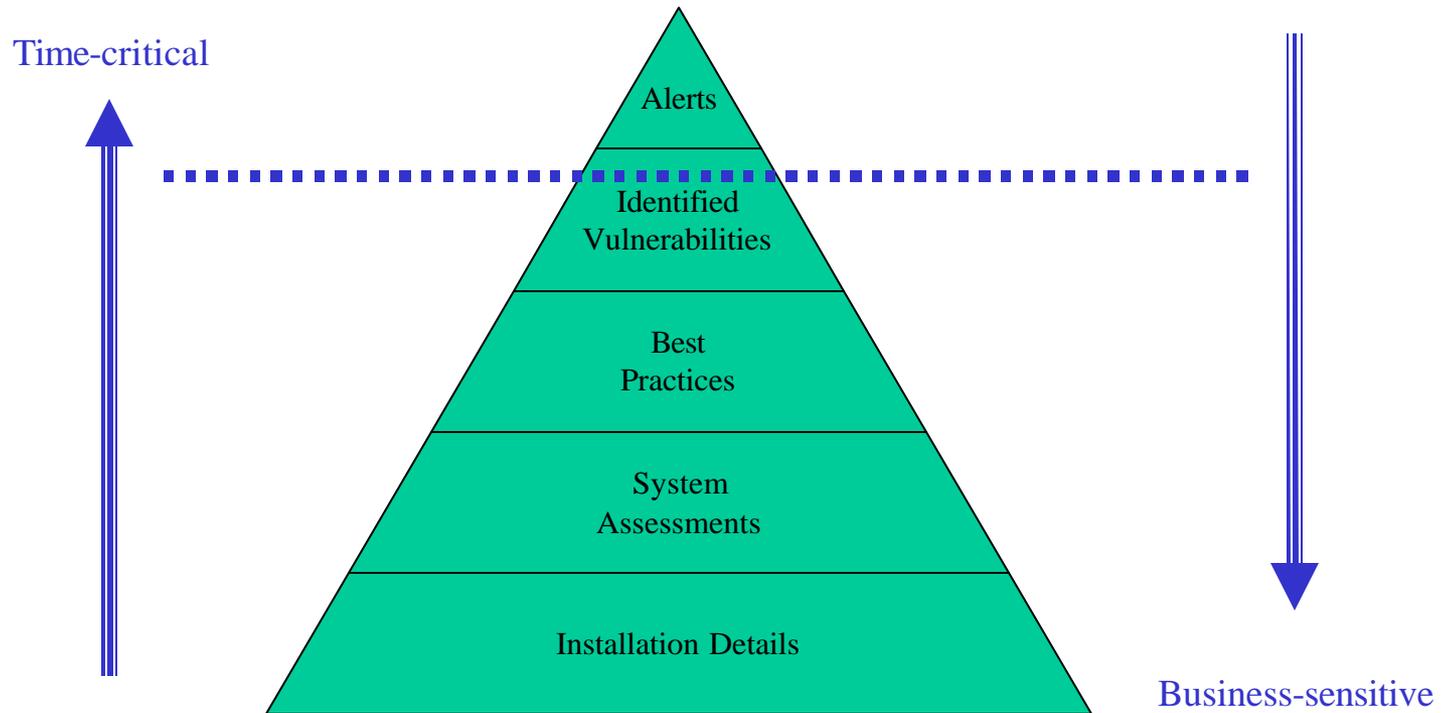
# Organizational Role Models for Information Sharing

- CERT and ISACs – Federally funded
- SANS – Private and Independent

# Legal Issues

- Business Proprietary
- Sharing with the U.S. Government
  - FACA
  - FOIA
  - PCII

# Information Sharing Iceberg



# Contact Information

Rita Wells

Critical Infrastructure Assurance

Advisory Engineer

(208) 526-3179

[rita.wells@inl.gov](mailto:rita.wells@inl.gov)