



Western Electricity Coordinating Council

# *CIP-007 Workshop*

---

WECC Critical Infrastructure Protection User Group (CIPUG)  
Marriott Mesa, Mesa, AZ  
January 20<sup>th</sup>, 2009

# *Disclaimer*

---

The Western Electricity Coordinating Council (WECC) makes no representation as to the accuracy or completeness of the information contained herein or otherwise provided by WECC, their affiliates or third parties, and accept no responsibility or liability, in contract, in tort, in negligence, or otherwise, should the information be found to be inaccurate or incomplete in any respect. WECC is not acting as an advisor to the recipient of this information, and the ultimate decision to proceed with any action rests solely with the recipient of this information.

Therefore, prior to entering into any action, the recipient of this information should determine, without reliance upon WECC, the economic risks and merits, as well as the legal, and accounting characterizations and consequences, of the transaction and that it is able to assume these risks.

# *Introduction*

---

- Thanks for coming!
- WECC staff are...
- Fire exits are...
- Restrooms are...
- Lunch will be around...
- Please use a microphone...
- Please silence all cell phones, mobile devices, laptops...

# WECC Outreach

---

- **J. Taud Olsen**

- *Director, Stakeholder Relations and Compliance Outreach*
- Office: 801.582.0353
- Direct: 801.819.7603
- Mobile: 801.883.6894
- [tolsen@wecc.biz](mailto:tolsen@wecc.biz)

- *And thanks to Kirha Quick and Bobbie Jessop for the logistics!*

# *CIP Audit Staff*

---

- **Bill Fletcher**

- wfletcher@wecc.biz
- 360.567.4061 (desk)
- 541.912.3226 (mobile)

- **Patrick Miller**

- pmiller@wecc.biz
- 360.567.4056 (desk)
- 503.260.6472 (mobile)

# *CIP Outreach Calendar*

---

- AC Workshop, Feb 10-11, Salt Lake City
  - CIP-002 Panel
  - WECC RBAM
  - First 13 AC Requirements
  - CIP Processes/Evidence 101
- CIP-008/009, March 18<sup>th</sup>, Boise
- CIP-003, April 14<sup>th</sup>, Denver
- CIP-004, May, Albuquerque?
- E-Sec/CIPUG – summer, Seattle?

# WECC CIPUG Workshops

---

- #1 request was for examples
  - WECC audit can't do that, but *you* can
- New CIPUG workshop model...
  - Asset owner volunteer panel walks through their organization's implementation
  - Industry expert panel of consultants and vendors provides feedback
  - Audience participation is strongly encouraged
- Webex suggestions?

# *Asset Owner Presenters*

---

- Chris Jager, Puget Sound Energy
  - Chair, E-Sec NW
- Mike Mertz, Southern California Edison
- Please thank them for volunteering for this event!

# *Industry Expert Panelists*

---

- Bryan Geraldo
- Matt Luallen
- David Baker
- Mel Drews
- Edward Vasko
- Michael Toecker
  
- Please feel free to approach them directly during breaks, lunch and after the event



Western Electricity Coordinating Council

# *CIP-007 Concepts and Facilities Sidebar*

---

Bill Fletcher, Compliance Engineer, Cyber Security  
bfletcher@wecc.biz  
360.567.4061

# Overview

---

- What are *Ports and Services*?
- What and where can I get unbiased information about them?

# *Ports and Services Terminology*

---

- Ports and Services - Go to the Source!
- Check back frequently
- Let's read as of ..... 01/13/09

*“ The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.*

*The Well Known Ports are those from 0 through 1023. DCCP Well Known ports SHOULD NOT be used without IANA registration. The registration procedure is defined in [RFC4340], Section 19.9. The Registered Ports are those from 1024 through 49151. DCCP Registered ports SHOULD NOT be used without IANA registration. The registration procedure is defined in [RFC4340], Section 19.9. The Dynamic and/or Private Ports are those from 49152 through 65535 A value of 0 in the port numbers registry below indicates that no port has been allocated.”*

Source - <http://www.iana.org/assignments/port-numbers>

# Ports and Services Terminology

\*\*\*\*\* \*

**PLEASE NOTE THE FOLLOWING:**

**\* \* \* IESG STATEMENT TO THE IANA**

**\* THE IESG BELIEVES THAT IANA MAY ALLOCATE AN ADDITIONAL PORT IN  
\* \* THE 'USER PORT' RANGE TO PROTOCOLS WHOSE CURRENT PORT ALLOCATION  
\* \* REQUIRES ACCESS TO A PRIVILEGED PORT. THIS ALLOCATION SHOULD NOT  
\* \* BE AUTOMATIC, BUT MAY OCCUR UPON APPLICATION BY AN INTERESTED  
\* \* PARTY WHOSE APPLICATION WOULD OTHERWISE FIT IANA'S POLICIES. \* \* \* \***

- 1. UNASSIGNED PORT NUMBERS SHOULD NOT BE USED. THE IANA WILL ASSIGN THE NUMBER FOR THE PORT AFTER YOUR APPLICATION HAS BEEN APPROVED.**
- 2. ASSIGNMENT OF A PORT NUMBER DOES NOT IN ANY WAY IMPLY AN ENDORSEMENT OF AN APPLICATION OR PRODUCT, AND THE FACT THAT NETWORK TRAFFIC IS FLOWING TO OR FROM A REGISTERED PORT DOES NOT MEAN THAT IT IS "GOOD" TRAFFIC. FIREWALL AND SYSTEM ADMINISTRATORS SHOULD CHOOSE HOW TO CONFIGURE THEIR SYSTEMS BASED ON THEIR KNOWLEDGE OF THE TRAFFIC IN QUESTION, NOT WHETHER THERE IS A PORT NUMBER REGISTERED OR NOT.**

\*\*\*\*\*

Source - <http://www.iana.org/assignments/port-numbers>

# Common Port-Based Protocols

---

- TCP      *Transmission Control Protocol*
- UDP      *User Datagram Protocol*
- DCCP     *Datagram Congestion Control Protocol*<sup>1</sup>
- SCTP     *Stream Control Transmission Protocol*<sup>1</sup>

Ports: The 16 bit number used by convention between remotely connected devices with a mutual desire to transmit binary information. Numerical Range: 0-65535<sup>2</sup>

Services: The (OSI) application layer function “listening” for connection requests on specific ports.

1. Relatively new protocols

2. Ports 0-1023 documented by IANA as “well-known” ports

# Protocol Basics

---

- TCP      *Some data integrity and reliability*
- UDP      *Data integrity only (unreliable over IPv4)*
- IP        Best effort, address-based, network layer
- TCP/IP    Used together, two different protocols

Ports: The 16 bit number used by convention between remotely connected devices with a mutual desire to exchange binary information. Numerical Range: 0-65535

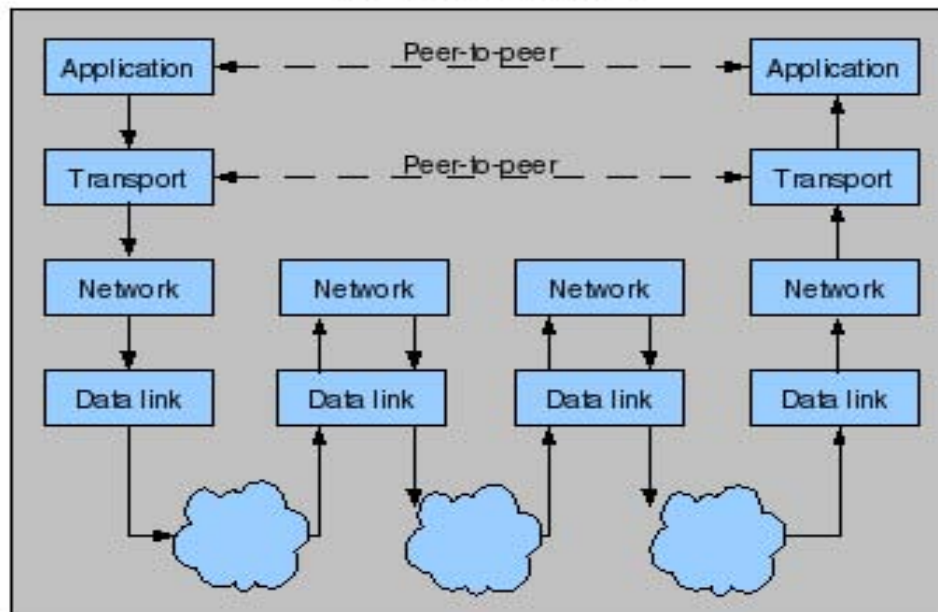
Services: The (OSI) application layer function “listening” for connection requests on a specific port.

# Protocol Basics

Network connections

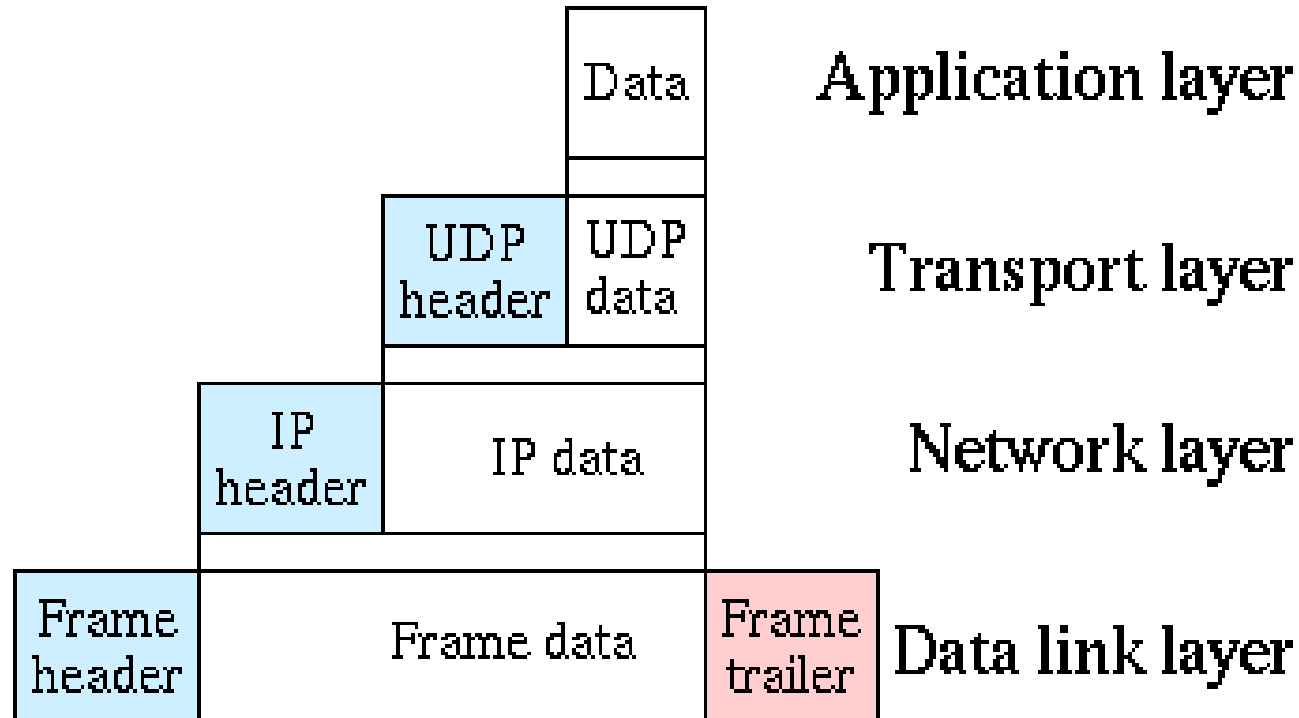


Stack connections



Source - Wikimedia Commons / Cburnett / GFDL 1.2

# TCP/UDP & IP Layering



Source - Wikimedia Commons / Cburnett / GFDL 1.2



# Selected Services and Ports

| Service (protocol) | Port                              | Protocol(s) |
|--------------------|-----------------------------------|-------------|
| telnet             | 23                                | TCP/UDP     |
| www (http)         | 80                                | TCP         |
| DNS                | 53                                | UDP         |
| Modbus/TCP         | 502 <sup>1</sup> (asa-appl-PROTO) | TCP         |
| ICCP               | 102 <sup>1</sup> (ISO-TSAP)       | TCP         |
| Ethernet/IP        | 44818 <sup>2</sup>                | TCP         |
| DNP/IP             | 20000 <sup>2</sup>                | TCP         |

<sup>1</sup> Unofficial re-use of IANA “Well-known” P/N Registry (0-1023)

<sup>2</sup> Listed in “Registered” segment IANA P/N Registry ( >= 1024)

# Academic Source

---

*“..The layering of protocols in critical infrastructure networks – exemplified by Modbus TCP in the oil and gas sector and SS7oIP in the telecommunications sector – raises important security issues. The individual protocol stacks, e.g., Modbus and SS7, have certain vulnerabilities, and transporting these protocols using carrier protocols, e.g., TCP/IP, brings into play the vulnerabilities of the carrier protocols. Moreover, the layering produces unintended inter-protocol interactions and, possibly, new vulnerabilities. This paper describes a formal methodology for evaluating the security of multilayer SCADA protocols. The methodology, involving the analysis of peer-to-peer communications and multilayer protocol interactions, is discussed in the context of Modbus TCP, the predominant protocol used for oil and gas pipeline operations... “*

Source: Public excerpt: Authors: Edmonds, Papa, Cheno, 2007

Ref: <http://www.springerlink.com/content/f88633252j015530/>

ISBN: 978-0-387-75461-1

# *Useful? Resources*

---

- <http://www.iana.org/assignments/port-numbers>
- [http://www.automation.schneider-electric.com/as-guide/EN/pdf\\_files/asg-9-industrial-networks.pdf](http://www.automation.schneider-electric.com/as-guide/EN/pdf_files/asg-9-industrial-networks.pdf)
- <http://blogfranz.googlecode.com/files/SCADA-Attack-Trees-IISW.pdf>
- <http://www.scadahoneynet.com/>
- <http://www.modbus-ida.org/tech.php>

## Note:

- Standard disclaimers apply
- Stay tuned to usual sources for late breaking information



Western Electricity Coordinating Council

# *CIP-007 Workshop*

---

WECC Critical Infrastructure Protection User Group (CIPUG)  
Marriott Mesa, Mesa, AZ  
January 20<sup>th</sup>, 2009

# Overview

---

- CIP-007 Schedule
- Spirit vs. Letter
- Architects vs. Auditors
- Evidence 101
- Self Reports and Mitigation Plans
- CIP-007 Vendor Group Question
- CSO706SDT

# *CIP-007 Schedule*

---

- Table 1
  - Part of the “First 13”
  - Compliant (C) by July 1<sup>st</sup>, 2008
  - Auditably Compliant (AC) by July 1<sup>st</sup>, 2009
- Table 2
  - Compliant (C) by July 1<sup>st</sup>, 2009
  - Auditably Compliant (AC) by July 1<sup>st</sup>, 2010
- Table 3
  - Compliant (C) by January 1<sup>st</sup>, 2010
  - Auditably Compliant (AC) by January 1<sup>st</sup>, 2011

# *Spirit vs. Letter*

---

- You will be audited against the letter, *but...*
- Immediately apparent or microscope?
- Keep it simple (Ockham's Razor)
- Keep it separate
  - Watch for dependencies
- Think beyond the letter
  - What if?
- Be prepared for investigations, just in case

# *Its All About...*

---

- The audit is not about...
  - The quality or security value of the design
  - Technology or platform preferences
  - Academics or theory
  - Probability, budget or convenience
- The audit is about...
  - Accountability
  - Transparency
  - Consistency
  - Sustainability

# *CIP Evidence 101 – Do*

---

- Evidence Dos:
  - Connect the dots in advance; try on my hat
  - Balance the details; moderation is good
  - Redact where appropriate
  - Common format
  - Human readable
  - Checksums (hashes; SHA256)
  - Automate whenever possible
  - Follow CIP-003.R4, R5

# *CIP Evidence 101 – Don't*

---

- Evidence Don'ts:
  - Please, no sensitive information without appropriate protections; **when in doubt, ask**
  - The “dump truck” factor
  - Is this the stuff you're looking for?
  - “Follow all NERC Regulations” bucket
  - Here it is, but you'll need *[insert proprietary product X]* to read it

# *CIP-007 Evidence*

---

- What type of evidence is best?
  - Yes. Yes it is.
  - No, really...
    - Word, Visio, Excel, PDF
    - System/event logs
    - Database reports
    - Packet captures
    - Observations
    - Pretty much anything

# *Third Party Resources*

---

- Be careful: time and money are scarce
- A well-crafted RFX can help
- Services
  - Everyone is an expert; ask around
  - ...it reminds me of a Dilbert cartoon
- Products
  - Nothing is 100%, all-in-one, total
  - Some options are emerging

# *Self Reports and Mitigation Plans*

---

- Violations are per Requirement
- Self Reports and Mitigation Plans can identify the Sub-requirement violated
- Be very clear and very detailed
  - Dates, systems, processes, etc mapped directly to the Requirement/Sub-requirement violated
- Don't forget to include the VRF (and VSL)!
- Provide ALL evidence necessary
- Again, be mindful of sensitive information

# CIP-007 Question

---

- Q1: Given CIP-007.R7, can an entity ship a device or data to a vendor for root cause analysis and/or troubleshooting?
- *A1: Yes. This requirement is specific to disposal and redeployment, and not analysis or troubleshooting. Please exercise caution and obtain all appropriate agreements and use a secure transfer method (adhere to CIP-003.R4).*

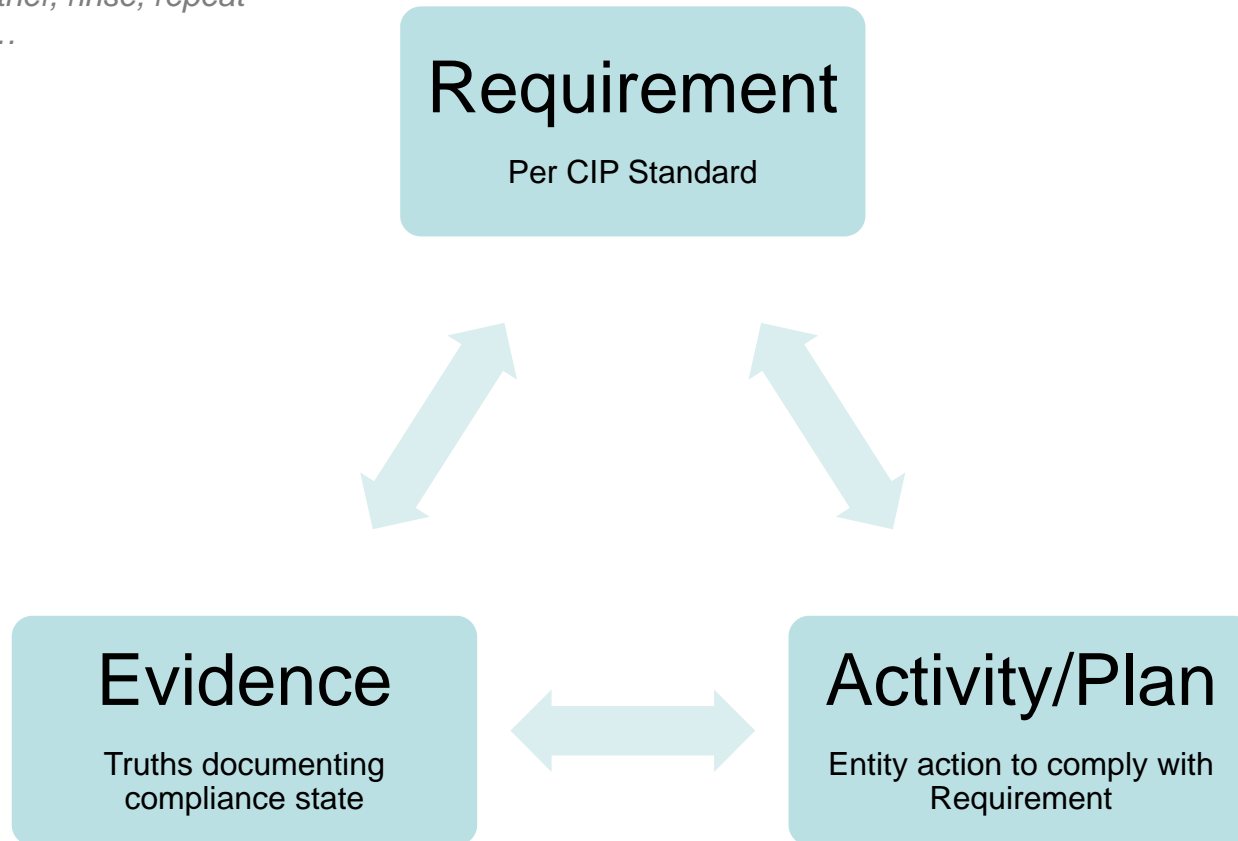
# CSO 706 SDT

---

- The CIP-007-02 Horizon
  - If you are still designing, factor in v2
  - If you are not still designing, start incremental changes to arrive at v2 on time
- Stay in the loop...
  - CSO706SDT “Plus” list
  - CIPC meetings
  - E-Sec NW, EEI, WICF, SANS, etc
  - Comment!

# Perpetual Compliance Cycle

*A.K.A. – lather, rinse, repeat  
or HWoD...*



# Questions?

---

**Patrick Miller CISA, CISSP-ISSAP**  
**Sr. Compliance Engineer, Cyber Security**  
**Western Electricity Coordinating Council**  
**7600 NE 41<sup>st</sup> Street, Suite 160**  
**Vancouver, WA 98662**  
**pmiller@wecc.biz**  
**503.260.6472 (m)**  
**360.567.4056 (d)**

**Bill Fletcher**  
**Compliance Engineer, Cyber Security**  
**Western Electricity Coordinating Council**  
**7600 NE 41<sup>st</sup> Street, Suite 160**  
**Vancouver, WA 98662**  
**wfletcher@wecc.biz**  
**541.912.3226 (m)**



Western Electricity Coordinating Council

# *CIP-007 Wrap-up*

---

Bill Fletcher, Compliance Engineer, Cyber Security  
bfletcher@wecc.biz  
360.567.4061

# *Language and Terminology*

---

- **CIP 007-1 / R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).**
- **NERC Glossary information – Cyber Asset:**  
Programmable electronic devices and communication networks including hardware, software, and data.

# Background Resources - R4/R5 Topics

---

- Whitelisting info: <http://en.wikipedia.org/wiki/Whitelist>
- Testing Methodology  
<http://www.breakingpointsystems.com/resources/testmethodologies/ips>
- Common Vulnerabilities and Exposures (CVE)  
<http://www.cve.mitre.org/compatible/product.html>
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling  
<http://csrc.nist.gov/publications/nistpubs/index.html>
- NIST SP 800-31, Intrusion Detection Systems  
<http://csrc.nist.gov/publications/nistpubs/index.html>
- Study by Gartner "Host-Based Intrusion Prevention Systems (HIPS) Update: Why Antivirus and Personal Firewall Technologies Aren't Enough"  
[http://www.gartner.com/teleconferences/attributes/attr\\_165281\\_115.pdf](http://www.gartner.com/teleconferences/attributes/attr_165281_115.pdf)
- Study by Gartner "Magic Quadrant for Network Intrusion Prevention System Appliances, 1H08"  
[http://www-935.ibm.com/services/us/iss/pdf/esr\\_magic-quadrant-for-network-intrusion-prevention-system-appliances-1h08.pdf](http://www-935.ibm.com/services/us/iss/pdf/esr_magic-quadrant-for-network-intrusion-prevention-system-appliances-1h08.pdf)
- Authentication Protocols: [http://en.wikipedia.org/wiki/List\\_of\\_authentication\\_protocols](http://en.wikipedia.org/wiki/List_of_authentication_protocols)

# Information Resources

---

- <http://www.iana.org/assignments/port-numbers>
  - [http://www.automation.schneider-electric.com/as-guide/EN/pdf\\_files/asg-9-industrial-networks.pdf](http://www.automation.schneider-electric.com/as-guide/EN/pdf_files/asg-9-industrial-networks.pdf)
  - <http://blogfranz.googlecode.com/files/SCADA-Attack-Trees-IISW.pdf>
  - <http://www.scadahoneynet.com/>
  - <http://www.modbus-ida.org/tech.php>
  - <http://www.dnp.org>
  - <http://www.odva.org/>
  - <http://seclab.uiuc.edu/docs/iccp-intro.pdf>
  - [http://www.nerc.com/files/Glossary\\_12Feb08.pdf](http://www.nerc.com/files/Glossary_12Feb08.pdf)
- Standard disclaimers apply. Some sites require membership.
- Stay tuned to usual sources for late breaking information.

# *Information Resources, continued*

---

- Some NIST Resources:

[http://nvd.nist.gov/images/cwe\\_cross\\_section\\_large.jpg](http://nvd.nist.gov/images/cwe_cross_section_large.jpg)

<http://csrc.nist.gov/groups/SNS/index.html>