



Idaho National Laboratory

# Vulnerability Disclosure

**Rita Wells**

National SCADA Test Bed DoE-OE

September 09, 2008

# Department of Energy-Office of Electricity Delivery and Energy Reliability: National SCADA Test Bed Program

## Mission

Support industry and government efforts to enhance control systems cyber security in the energy infrastructure



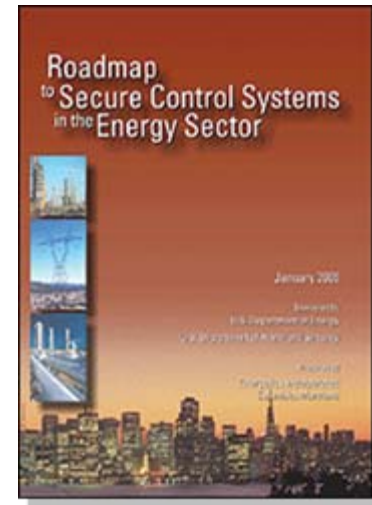
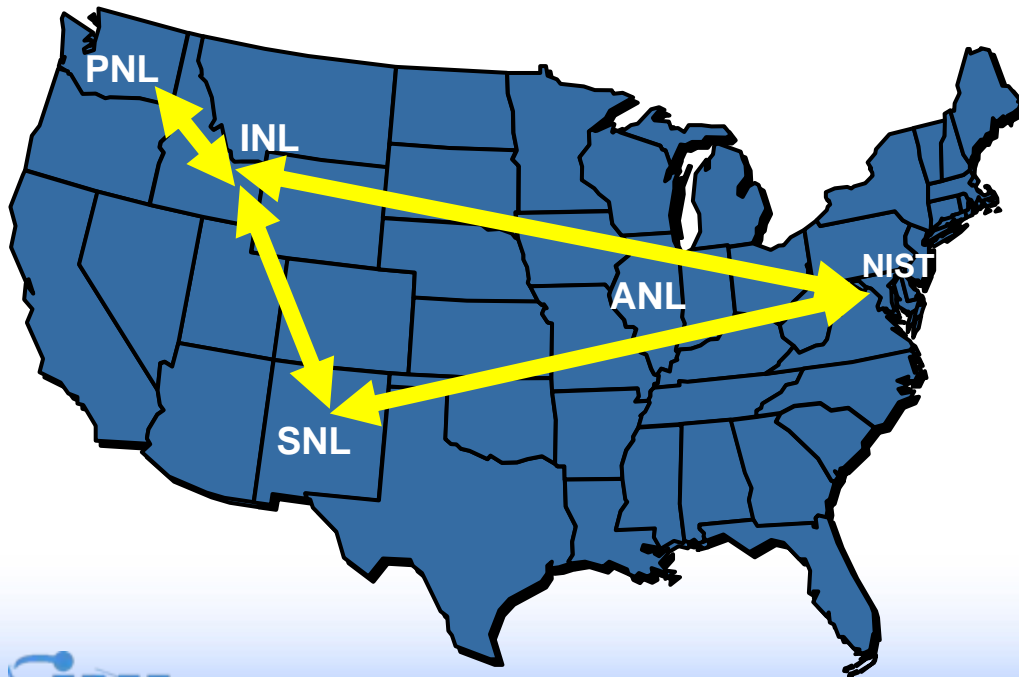
**Key INL activities** are **cyber Vulnerability Assessments** (testing) and **Industry Outreach** (including training)

Over 22 assessments in lab and on site ranging from 275 to 800 hours of cyber security researchers in addition to control systems and network engineer hours per each assessment  
Common vulnerabilities analyzed

# National SCADA Test Bed

*DOE multi-laboratory program designed to:*

***Support industry and government efforts to enhance control systems cyber security across the energy infrastructure***



## Key Program Areas

- Assess and mitigate energy control systems vulnerabilities*
- Develop advanced secure control systems technologies*
- Support development of standards and best practices*
- Conduct outreach and awareness*

# Vulnerability Disclosure – Government Sponsored

Time to public disclosure for CERT/Coordinating Center (CERT/CC) is normally 45 days

- More serious vulnerabilities are coordinated with US-CERT for disclosure<sup>[1]</sup>
- Trending of Vulnerabilities



From the FAQ: Our work is funded primarily by the U.S. Department of Defense and the Department of Homeland Security, along with a number of other federal civil agencies.

[1] CERT/CC Vulnerability Disclosure Policy, [http://www.cert.org/kb/vul\\_disclosure](http://www.cert.org/kb/vul_disclosure) Cataloged vulnerabilities

Year	Total vulnerabilities cataloged	From direct reports
Q1-Q2, 2008	4,110	196
2007	7,236	357
2006	8,064	345
2005	5,990	213
2004	3,780	170
2003	3,784	191
2002	4,129	343
2001	2,437	153

# Vulnerability Disclosure – Government Sponsored - continued

---

The US-CERT time to disclose varies for control systems based vulnerabilities

- US-CERT provides a more timely alert to control system vulnerabilities to users that register for through the secure portal
- While other more IT centric vulnerabilities are published the same day as public disclosure

The CitectSCADA buffer overflow ([VU#476345](#)) vulnerability it was one month from public disclosure to US-CERT published notes

[http://www.kb.cert.org/CERT\\_WEB/services/vul-notes.nsf/id/476345](http://www.kb.cert.org/CERT_WEB/services/vul-notes.nsf/id/476345)



# Vulnerability Discovery - Who

---

- **Security Firms** – Core Security discovered two Citect vulnerabilities and one Wonderware vulnerability this year

<http://www.coresecurity.com/index.php5?module=ContentMod&action=item&id=2312>

- **Hackers** – OPC vulnerability at BlackHat 2007

<http://www.eweek.com/c/a/Security/Hole-Found-in-Protocol-Handling-Vital-National-Infrastructure/>

- **Protected Entities** – DHS-NCSD-CSSP Control System Security Program and DOE-OE National SCADA Test Bed and others
- **Vendor** – Rarely disclosed prior to release notes
- **End User** – Disclosed to Vendor

# Stakeholders Perspectives

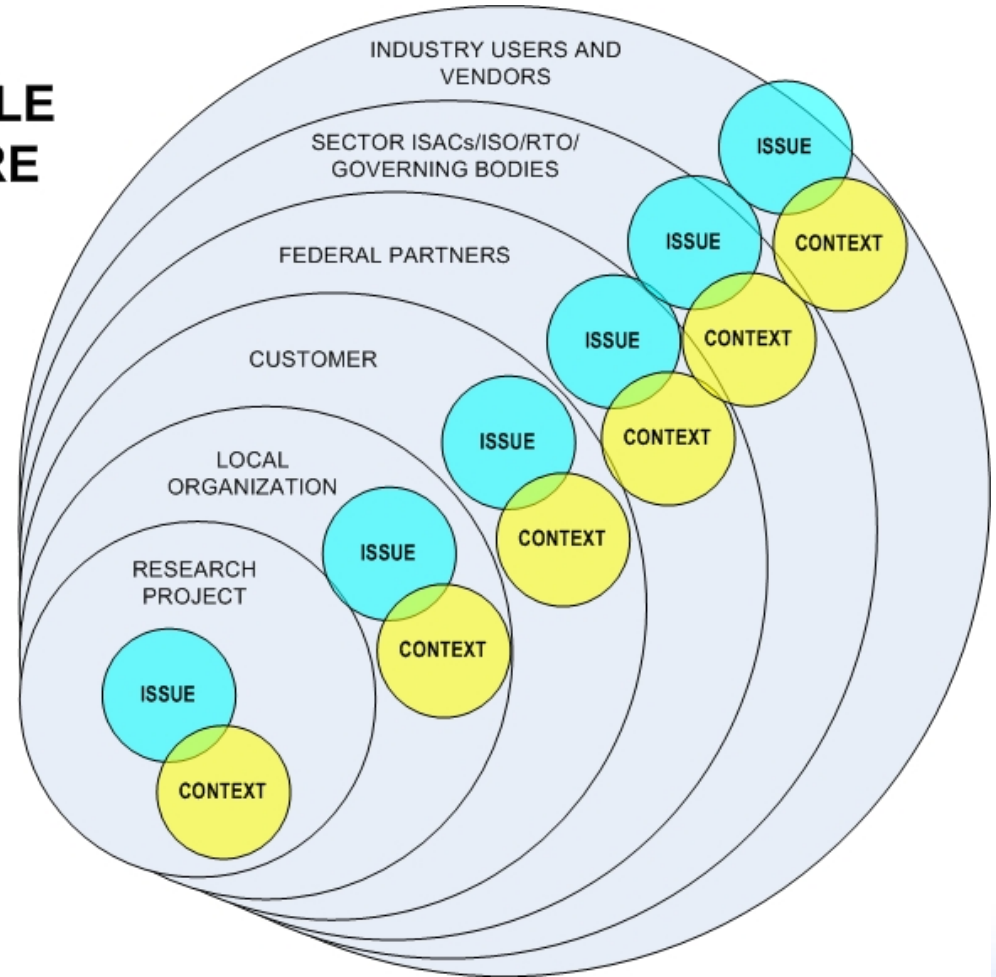
---

- Discoverer – wants disclosure or not
- Vendor – varies on culture normally all share with customers after fix
- Government – Want to promote better secure systems while protecting infrastructure owned by private entities
- End User – want to know prior to mitigations developed to apply defense in depth or other temporary protections

# Responsible Disclosure

## RESPONSIBLE DISCLOSURE

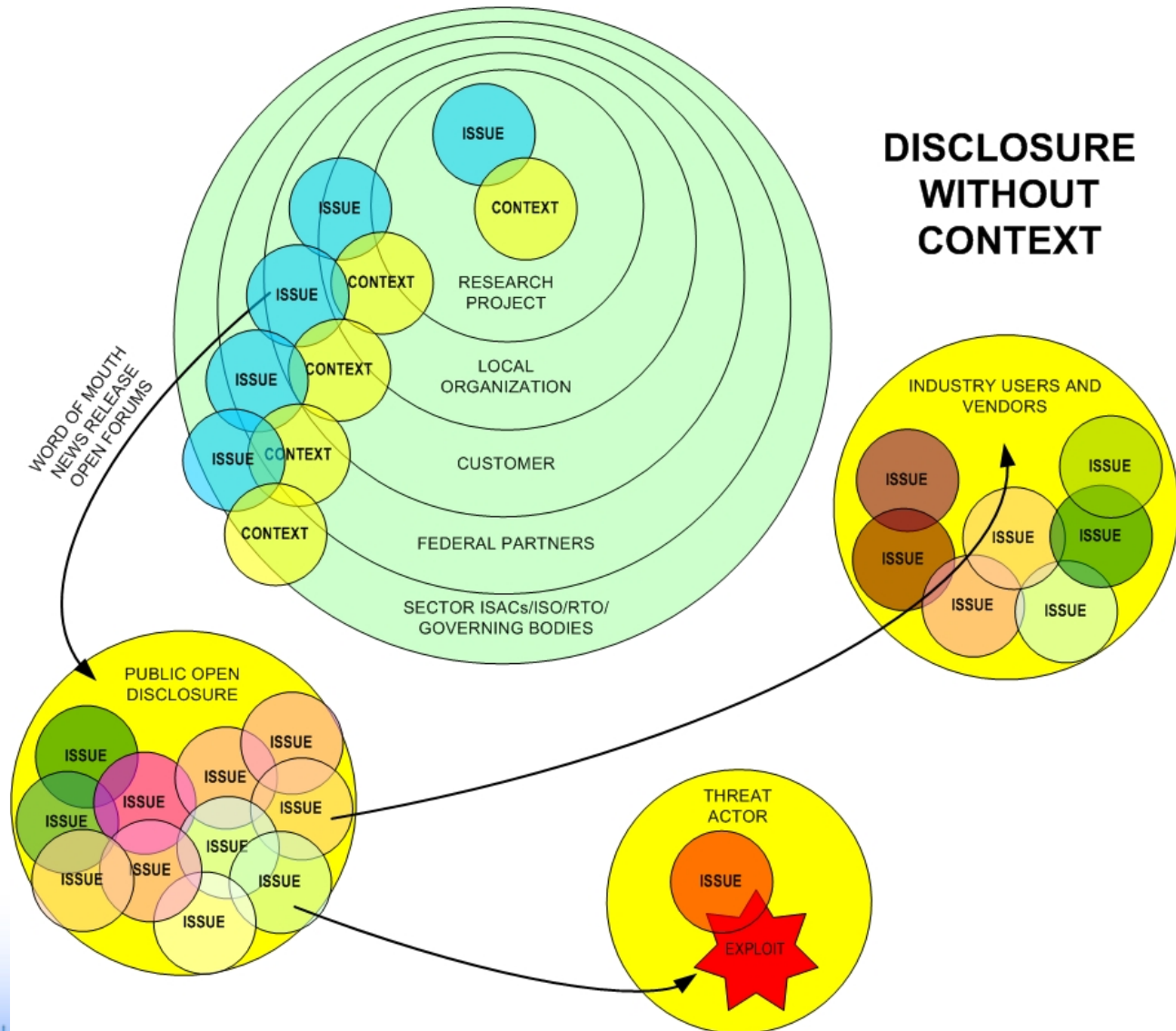
**Context and vulnerability issue are coupled**





# Responsible Disclosure

- Vulnerability Issue gets more attention and strays from context

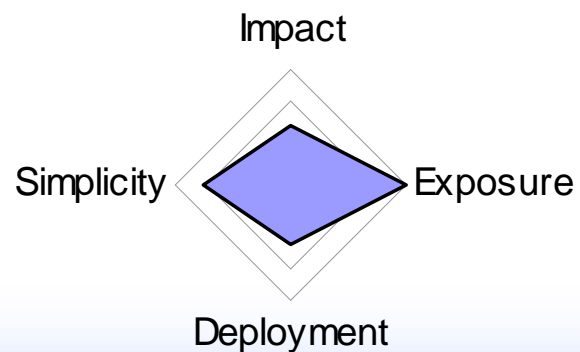


# Vulnerability Characterization

## Attack Surface Example

- Impact (Medium) will cause a denial of service (crash) if successfully exploited
- Exposure (High) can be exploited by an unauthenticated attacker having network access only
- Deployment (Medium) exists in a configuration that is present in some U.S. critical infrastructure control system applications
- Simplicity (Moderately High) has its exploit code publicly available for use with automated exploit tools

■ EXAMPLE (CVE-2006-3942)










# Concluding Recommendations

---

- Use disclosure process that includes context and characterization of the vulnerability
- Asset owners need to do their own characterization of vulnerabilities specific to architectures
- Mine the large knowledge base of vulnerabilities for control systems
- Create more independent and open testing facilities
- Require government co-sponsored testing to open up information after aged
- Analyzed aged information for trending back to asset owners

# Resources Available


Address  <https://portal.us-cert.gov/member/mail3/index.cfm?gotomsgid=325547&compartmentP=1124511>   Go  Links  Customize Links  Free Hotmail

 **US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

NC4 Support Center  
(866) 827-6201  
helpdesk@nc4.us

**Secure Portal User Login**

**ATTENTION:**  
**This system contains U.S. Government Data.**  
Unauthorized use of this system is prohibited.




Username:

Password:

This system contains data belonging to the U.S. Government. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. U.S. Government computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this computer system, authorized or unauthorized, constitutes

 **US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM  
[Home](#) -> [Library](#)

NC4 Support Center: (866) 827-6201  
email: helpdesk@nc4.us

**Control Systems Center**

# Contact Information

---

Dave Kuipers  
National SCADA Test Bed  
INL Program Manager  
208-526-4038  
[david.kuipers@inl.gov](mailto:david.kuipers@inl.gov)

Rita Wells  
208-526-3179  
[rita.wells@inl.gov](mailto:rita.wells@inl.gov)