



**Electric Industry**  
Regulatory Solutions

# Electric Sector Security Crystal Ball

---

**Is Security In Your Future?**

---

EnergySec Summit, Denver, CO  
09/21/2010

Cybersecurity Solutions  
[www.icfi.com/cyber](http://www.icfi.com/cyber)





Security and  
Emergency  
Management



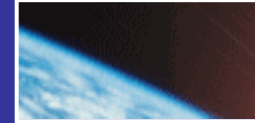
Information  
Technology



Transportation



Energy



Environment



Economic  
Development

Service  
Areas

## Strategy

Market and Policy Analysis

Technology Assessment

Program and Project Management

Enterprise Information Technology Solutions

Human Capital Management

Strategic Communications

Clients

Government

Civilian / Defense  
Homeland Security



Industry

Transportation  
/Energy /Other



# Qualifications, Past Performance, and Differentiators



ICF Cyber Security Team	INDUSTRY EXPERTISE & METHODOLOGY QUALIFICATIONS						
	GO / TO	Fortune 500	NERC CIP / ISO Standards	NIST SP 800-53	RBAM Methods	Control System Vendors	SANS SCADA Training
	✓	✓	✓	✓	✓	✓	✓

*Assessment and Implementation Experience*



### Strong Performance Record:

- ✓ **Building** NERC CIP Cyber Security Programs
- ✓ **Assessing** NERC CIP Control Effectiveness
- ✓ **Recommending** Compliance Program Enhancements

Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.



# Introduction

- Patrick C Miller
  - Director - NERC CIP Practice, ICF International
  - Former WECC Manager of CIP Audits & Investigations
  - Former Chair and founder, EnergySec
  - Worked for several asset owners in WECC
  - 13 years in Electric Power sector
  - CRISC CISA CISSP-ISSAP SSCP CEH CVI NSA-IAM



## Reliability Will Be Misrepresented

- Mom, Uncle Sam and Apple Pie are noble causes but reliability is really about money
  - Rate recovery, profits, politics, lawsuits, brand value, stock price...
  - Public boards, politics, sustainable rates, lawsuits, upstream energy markets...
  - Other economic impacts (how much did the August 2003 blackout cost?)...

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Attackers Will Maintain The Advantage

- Security approaches favor new installations, legacy environments are still vulnerable
- Very difficult to replace in-service devices
- Stuxnet: game changer, even when sophisticated attacks aren't necessary
- Organized crime will top Nation States and NGOs as biggest threat

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



# The Limelight Will Get Brighter

- Electric sector (SCADA) = new shiny object
- TV, movies, media, blogosphere, Twitter
- Armchair experts and hyperbole
- Other critical infrastructures, nation states
- The mania will intensify in the near term
- Very little actuarial data to form risk models

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Rescue Is Not Coming Soon

- Not enough qualified security pros are available
- Very complex range of skills needed
- New talent is being trained
  - Academic vs. in-the-field experience
  - Training options are limited and/or questionable
- Technical training available, but little or none for soft skills

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## New Technology Won't Help

- ARRA and other “green” dollars are flowing
- \$AnySCADA device, now with a flash-webserver-WiMax-mesh-ZigBee-kitchensink
- Logical distance between kinetic endpoint and HMI is exponentially increasing
- Most vendors put features first, security last; this will not change in the foreseeable future

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Vendor Relationships Will Change

- SCADA Procurement Language
- Security testing in FAT, and again in SAT
- Code reviews are still an option
- 100% total absolute comprehensive über secure will never exist
- Bandolier, Achilles, etc
- Coordinated disclosure

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Incident Response Will Improve

- Prevention gets the most weight now, but...
- When breached, do you rebuild/replace or operate with diminished integrity assurance?
  - How long can you operate without assurance?
  - Is there spare equipment on eBay?
  - Can you take an outage?
- Forensics will be particularly challenging



## Regulation Will Get Muddy

- Accountability baseline still forming
- Consensus is not possible; ANSI flaws
- Why are there 3 different security standards?
- Region/NERC/FERC relationship is unstable
- Data breach laws are likely
- Overlapping regulations (SOX, CFATS, MTSA...)
- Heavy politics attached to grid security

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Security And Compliance Will Clash

- Too many cases of lowering security to achieve strict compliance to NERC CIP standards
- The initial numbers aren't good: too few Critical Assets and Critical Cyber Assets
- CIPS is more about accountability than security
- Future changes to CIPS are slow and inadequate
- Industry is actively trying to minimize

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



## Recommendations

- Prepare for the spotlight and microscope
- Be secure first, compliant second but don't ignore the regulatory landscape
- Realize that you are a target and act accordingly
- Get or grow the skills needed to protect you
- Money talks, vendors will listen
- Balance prevention and resilience/response

*Use or disclosure of data contained on this sheet is subject to the restrictions on the title page of this presentation.*



**Electric Industry**  
Regulatory Solutions

# Questions?

Patrick C Miller

Director, NERC CIP Practice

[pmiller3@icfi.com](mailto:pmiller3@icfi.com)

503-887-5497

---

Cybersecurity Solutions

[www.icfi.com/cyber](http://www.icfi.com/cyber)

---

**About ICF International:** ICF International (NASDAQ: ICFI) partners with government and commercial clients to deliver consulting services and technology solutions in the energy, climate change, environment, transportation, social programs, health, defense, and emergency management markets. Since 1969, ICF has been serving government at all levels, major corporations, and multilateral institutions. More than 3,500 employees serve these clients worldwide.



**Passion. Expertise. Results.**