EnergySec
National Electric Sector Cybersecurity Organization

Grid Modernization: Threats, Vulnerabilities and Security Challenges

December 8 2011
Grid-Interop
Phoenix Convention Center
Phoenix, AZ

Advantage: Adversaries

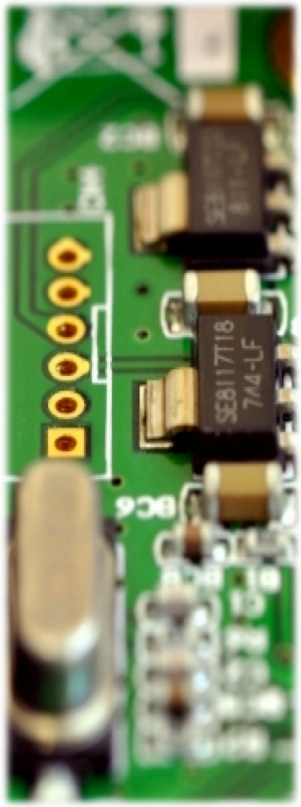
Motivated adaptive adversaries exist, and they don't follow the rules or compliance checklists

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Advantage: Adversaries

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Technology Landscape



- Emergent intelligence
- A new digital world order
- Widespread connectivity
- Size matters & doesn't
- Hyper-embeddedness
- Lingering legacy

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Policy Landscape

- Smart Grid interoperability
- Compliance vs. Security
- White House proposals
- Data breach disclosure
- Vendor, utility responsibility
- Intelligent islanding

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Cybersecurity Landscape

- Research, espionage, organized crime, warfare
- Nation state quality defense is the new normal
- Isolation is extremely difficult
- Bolt-ons are complex
- Cyber-kinetic impacts

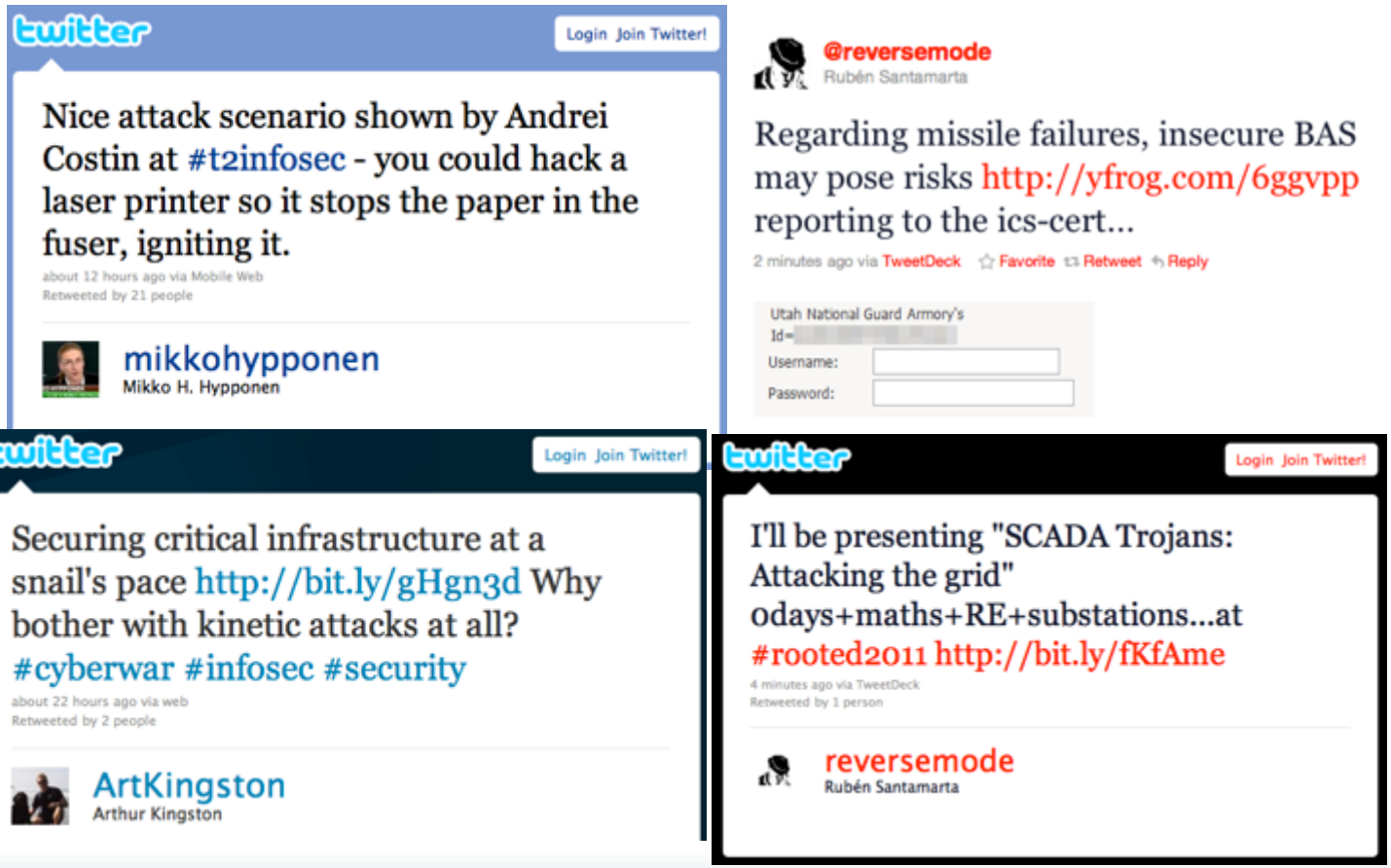
The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Cybersecurity Landscape

- Stuxnet
  - 5.74M Google hits
  - "Most sophisticated malware…"
  - "Game changer…"
- Duqu
  - 2.61M Google hits
  - Industrial equipment target

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Threat Landscape

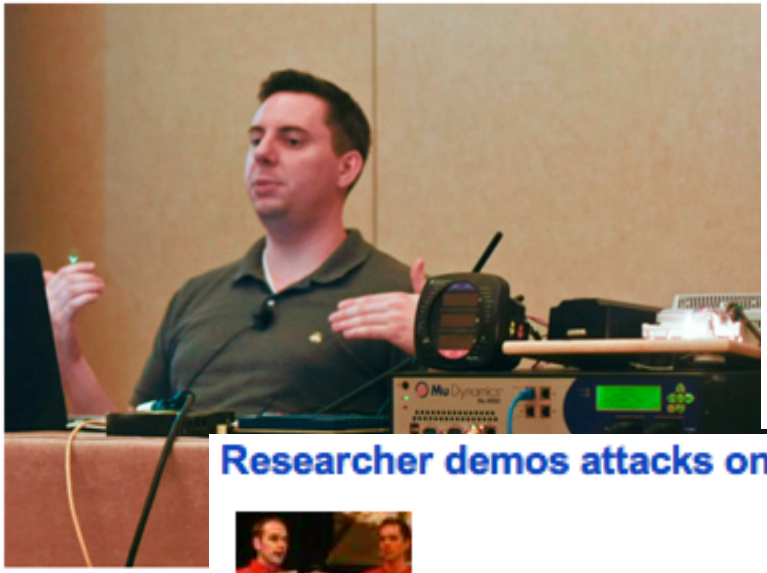


The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Threat Landscape

Google search opens SCADA systems to doomsday scenarios

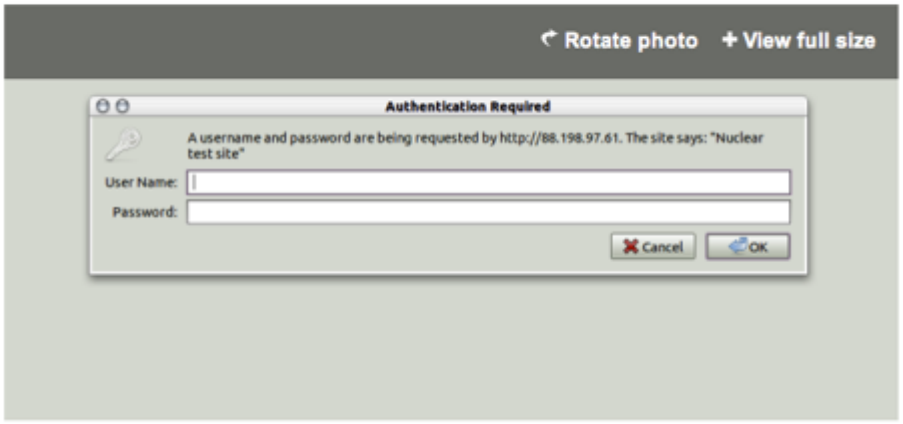
By Joseph Volpe posted Aug 4th 2011 5:26AM



Google, the service so great
The search site played inad
(SCADA) systems in a Black
CTO walked attendees thro

@krypt3ia
krypt3ia **October 7, 2011**

Tweet 0



Uhhhh.... #shodan

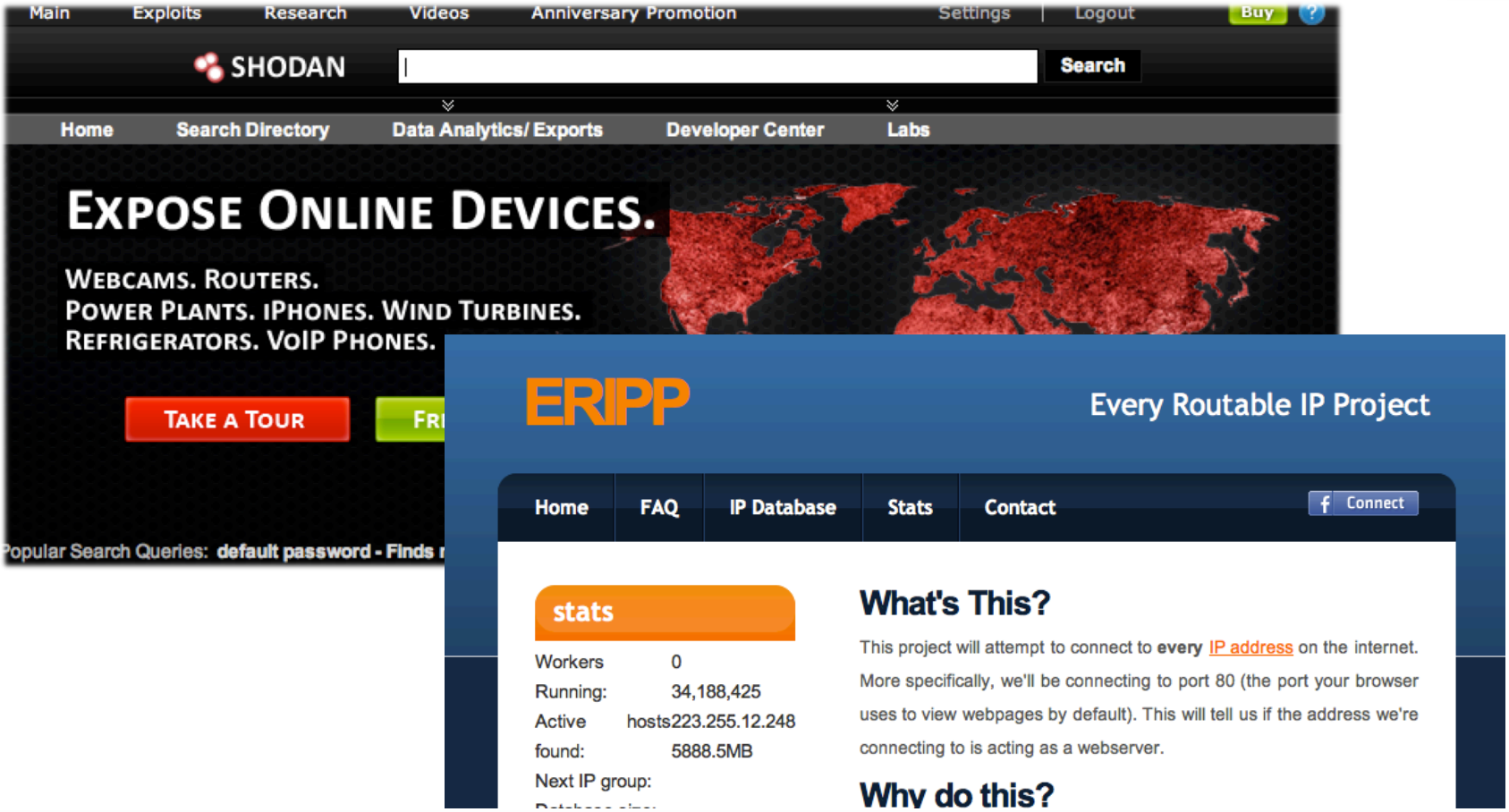
Researcher demos attacks on Siemens industrial control systems - CNET

CNET

Researcher demos attacks on Siemens industrial control systems
CNET
The protocol was intended to be open and packets are sent in plain text, he said, echoing concerns voiced by Jonathan Pollet, founder of Red Tiger Security, and Tom Parker, chief technology officer of FusionX, in their **SCADA** security workshop earlier ...
How easily can a power plant be hacked? Verymsnbc.com

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Vulnerability Landscape



The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Vulnerability Landscape

69.92.101.2
Added on 10.02.2011

69-92-101-2.cpe.cableone.net

HTTP/1.0 **200** OK
Server: **LV_HTTP**/1.0
Date: Thu, 10 Feb 2011 07:35:23 GMT
Content-type: text/html
Last-modified: Wed, 25 Jan **200**6 20:41:17 GMT
Content-length: 704

69.139.97.213
Added on 09.02.2011

c-69-139-97-213.hsd1.ms.comcast.net

HTTP/1.0 **200** OK
Server: **LV_HTTP**/1.0
Date: Wed, 09 Feb 2011 15:49:33 GMT
Content-type: text/html
Last-modified: Wed, 25 Jan **200**6 20:41:17 GMT
Content-length: 704

66.212.169.244
Added on 09.02.2011

dl.cashcode.com

HTTP/1.0 **200** OK
Server: **LV_HTTP**/1.0
Date: Wed, 09 Feb 2011 08:20:09 GMT
Content-type: text/html
Last-modified: Tue, 05 Aug **200**3 14:42:04 GMT
Content-length: 1041

139.6.18.127
Added on 01.02.2011

ntrt127.ntl.FH-Koeln.DE

HTTP/1.0 **200** OK
Server: **LV_HTTP**/1.0
Date: Tue, 01 Feb 2011 16:24:22 GMT
Content-type:
Content-length: 580

96.11.251.66
Added on 13.08.2010

rrcs-96-11-251-66.central.biz.rr.com

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: **Ubicom**/1.1
Content-Length: 26
WWW-Authenticate: Basic realm="(Tenn-**Plant**)"
Connection: close

64.7.227.38
Adtran NetVanta
Added on 25.05.2010

HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: **Ubicom**/1.1
Content-Length: 26
WWW-Authenticate: Basic realm="(Wnsbro Water **Plant**)"
Connection: close

209.47.163.29
Adtran NetVanta
Added on 15.04.2010

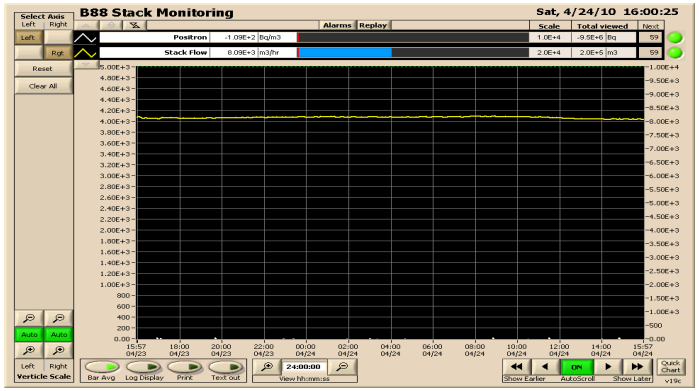
HTTP/1.0 401 401 Authorization Required
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Server: **Ubicom**/1.1
Content-Length: 26
WWW-Authenticate: Basic realm="(water-**plant**-ap)"
Connection: close

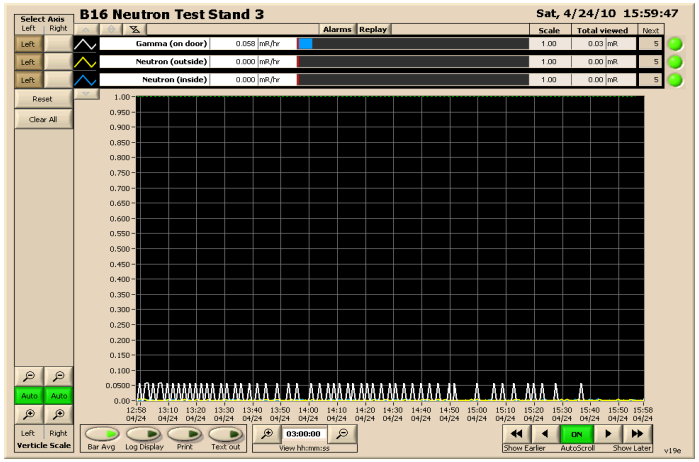
69.43.15.180
Added on 19.11.2009

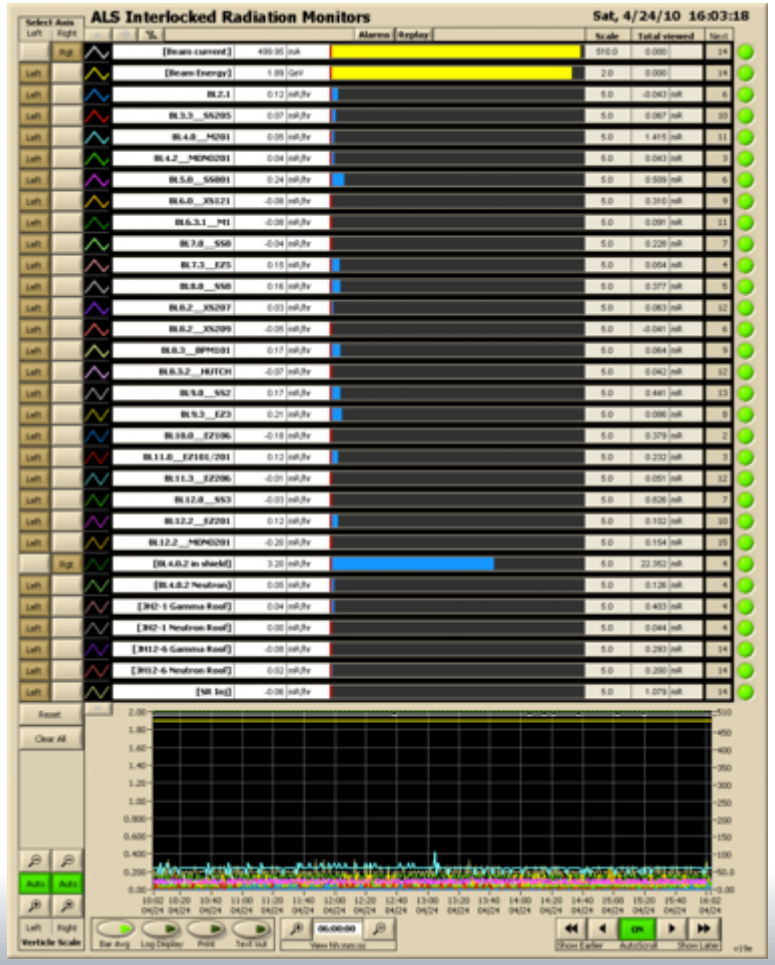
HTTP/1.0 401 401 Authorization Required
Content-length: 26
Expires: Thu, 1 Jan 1970 00:00:01 GMT
Server: **Ubicom**/1.1
Connection: close
Pragma: no-cache
Cache-control: no-cache, no-store, must-revalidate, max-age=0
Www-authenticate: Basic realm="(Waverly Water **Plant**)"

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Vulnerability Landscape





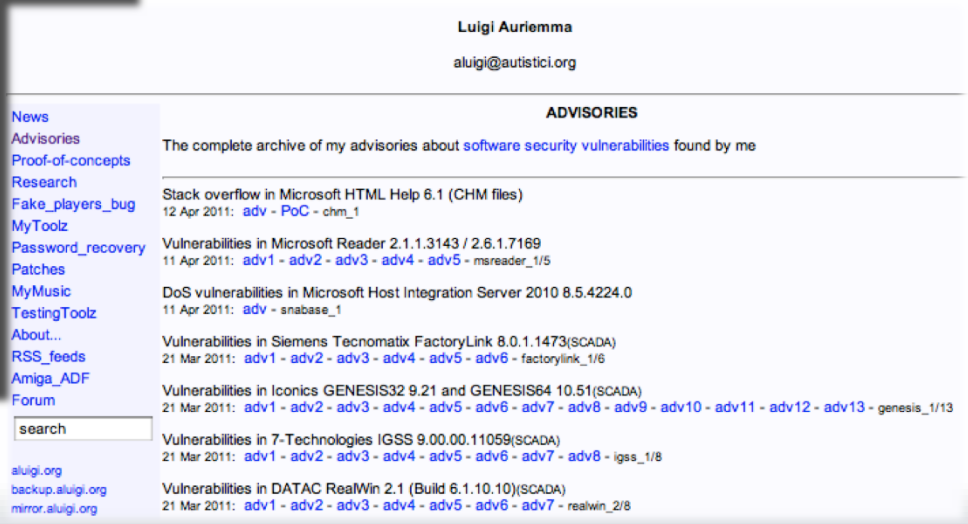


Berkeley Cyclotron HMI images

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Vulnerability Landscape

46 zero-day SCADA vulnerabilities issued a two-week span



The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

From Obscurity To Novelty

- Smart Meter ($device) hacking is trendy
- Sophisticated, easy-to-use hacking toolsets are freely available on the Internet
  - Cookbooks, fuzzers, sniffers, Metasploit
- Supply chain attacks
- Manuals available in all languages on Internet

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Today's Shiny Object

- Headline presentations at security events
  - BlackHat, DefCon, DerbyCon, RootedCon…
- Mainstream media
  - Wall Street Journal, Bloomberg, CNN
- Too many industry trade publications to name
- Blockbuster films, prime time TV shows
- Person-on-the-street, Congress, White House

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Perspective & Solutions

- Sufficient MMO exist for potential impacts to Energy infrastructure elements
- Adversaries will easily outpace regulation, procurement and implementation cycles
- Balance prevention, detection and response (drills, exercises)
- People first, technology second
- The Aware Person System (APS)

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

National Electric Sector Cybersecurity Organization

- EnergySec awarded funding assistance from DOE to establish the National Electric Sector Cybersecurity Organization (NESCO)
- NESCO Mission:
  - Lead an independent, broad-based, public-private partnership to improve electric sector energy systems cyber security
  - Become the security voice of the electric sector

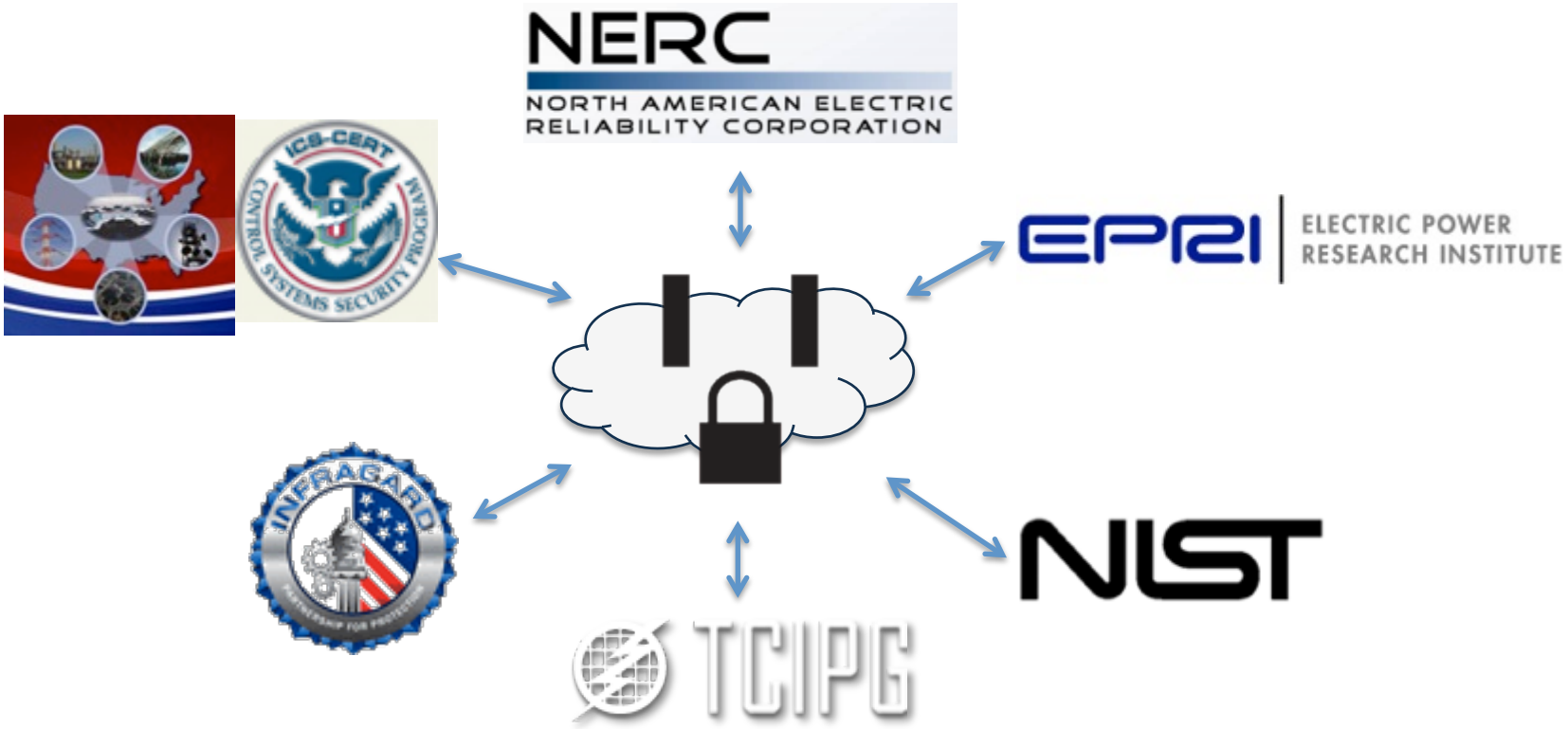
The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

NESCO Objectives

- Identify & disseminate common effective cyber security practices
- Analyze, monitor & relay threat information
- Focus cybersecurity R&D priorities
- Work with federal agencies to improve electric sector cybersecurity
- Encourage key electric sector vendor support & interaction
- Connect/harmonize all of the existing cybersecurity efforts & minimize duplication

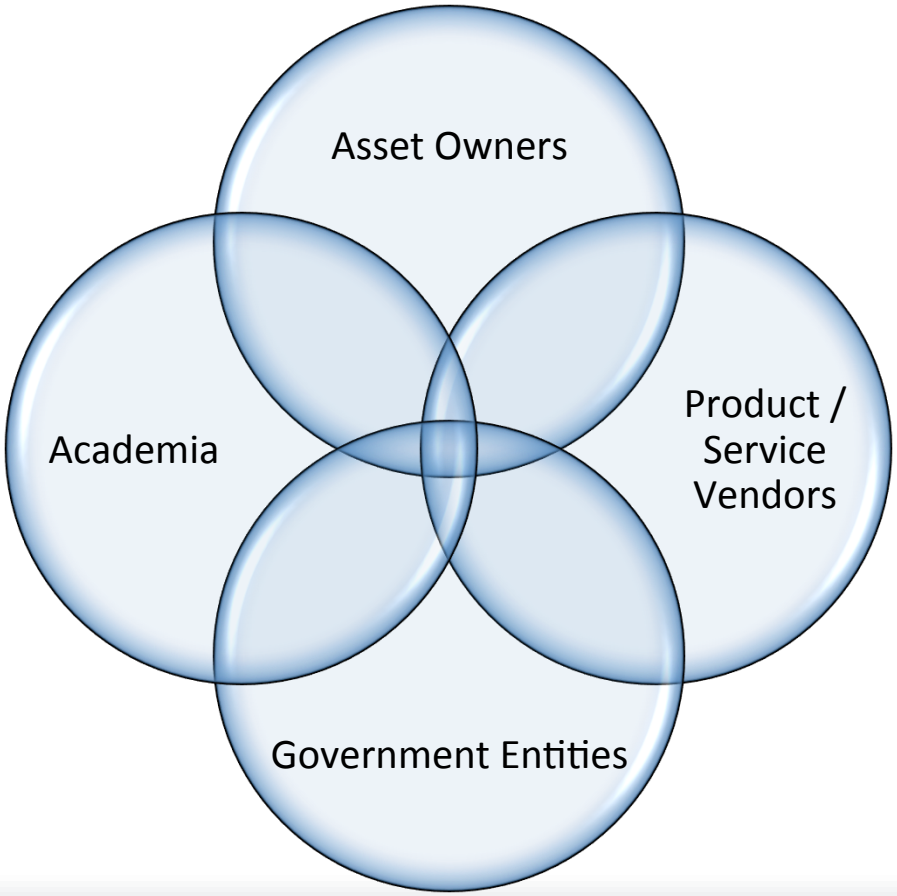
The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Connect & Support



The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Industry Collaboration



The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Unique and Independent

- Managed and operated by EnergySec
- Built on foundation of 10 years of experience
- Independent 501(c)(3) nonprofit
- First of its kind public-private partnership
- 3 years of DOE funding assistance: 60/40
- Strong and diverse leadership
- Strong and diverse membership

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Engage Equip Empower

- Sharing requires trust
- Trust is built on relationships
- Our approach…
  - Bringing people together
  - Flexible technology options and solutions to extend and enhance relationships

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

One Drop of Water...

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

National Electric Sector Cybersecurity Organization

Plug In

www.energysec.org/nesco

Patrick C Miller
President & CEO, EnergySec
Principal Investigator, National Electric Sector Cybersecurity Organization
patrick.miller@energysec.org
503.446.1212 (desk)
@patrickcmiller (twitter)
www.energysec.org

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.