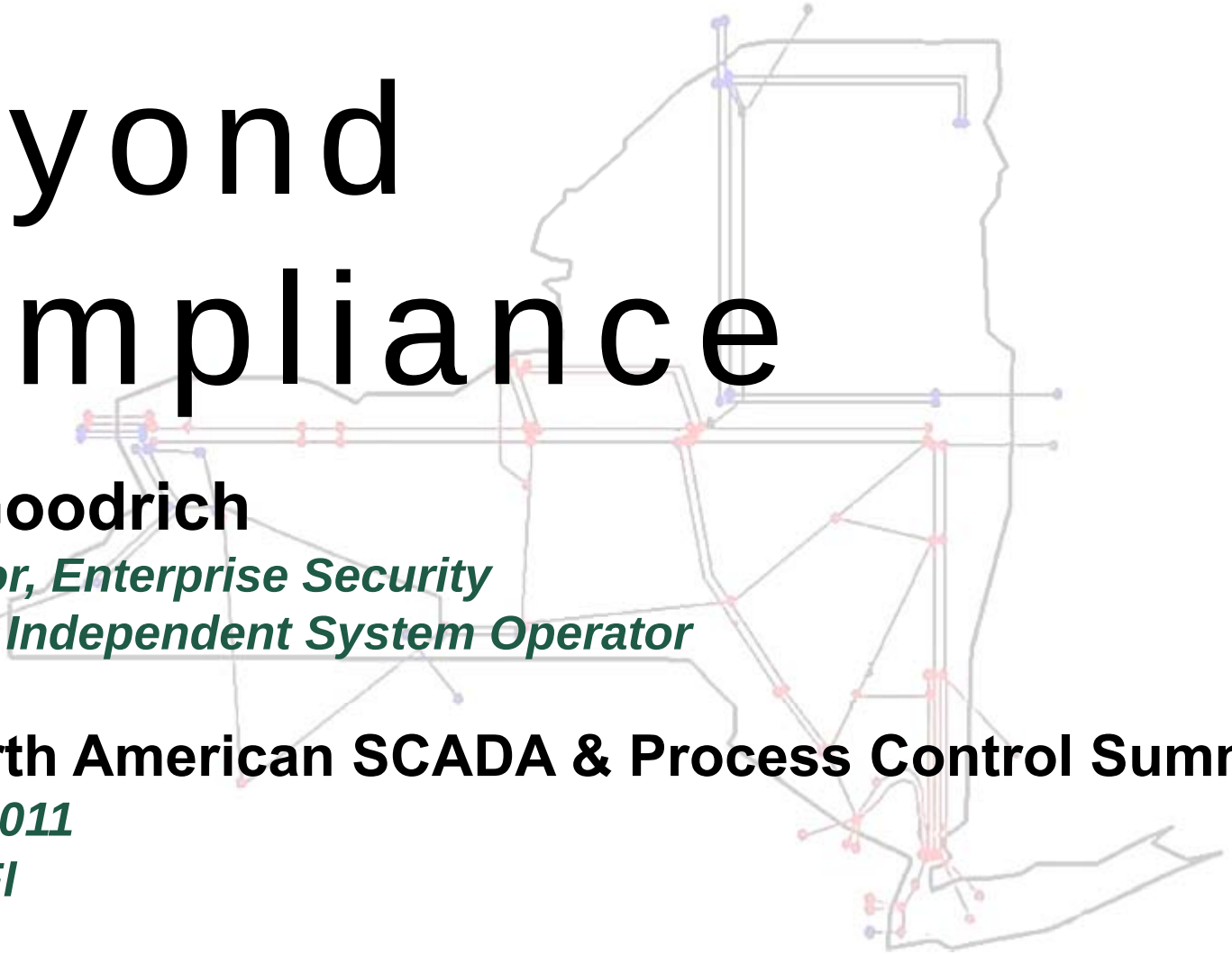
Beyond Compliance



Greg Goodrich
Supervisor, Enterprise Security
New York Independent System Operator

2011 North American SCADA & Process Control Summit
March 1, 2011
Orlando, Fl

Roles of the NYISO

Reliable operation of the bulk electricity grid

- ***Managing the flow of power over nearly 11,000 circuit-miles of transmission lines from more than 300 generating units***

Administration of open and competitive wholesale electricity markets

- ***Bringing together buyers and sellers of energy and related products and services***

Planning for New York's energy future

- ***Assessing needs over a 10-year horizon and evaluating projects proposed to meet those needs***

Advancing the technological infrastructure of the electric system

- ***Developing and deploying information technology and tools to make the grid smarter***

Agenda

- **Compliance ↔ Security**
- **Processes ↔ People**
- **Assets ↔ Environments**
- **Examples**
- **Resources**

I heard this statement:

- Compliance is the floor you land on when your security is tripped.

  (*Author unknown*)

- Makes you think...
- Defense In Depth

Compliance….

Compliance .vs. Security

- Compliance=Risk
- Compliance>Quantify
- Security=Risk
- Security<Quantify

Compliance <==> Security

- In the open source world, comments are required and make it better
- Documenting compliance supports security
- Demonstrate security by documenting and thus demonstrate compliance

Processes

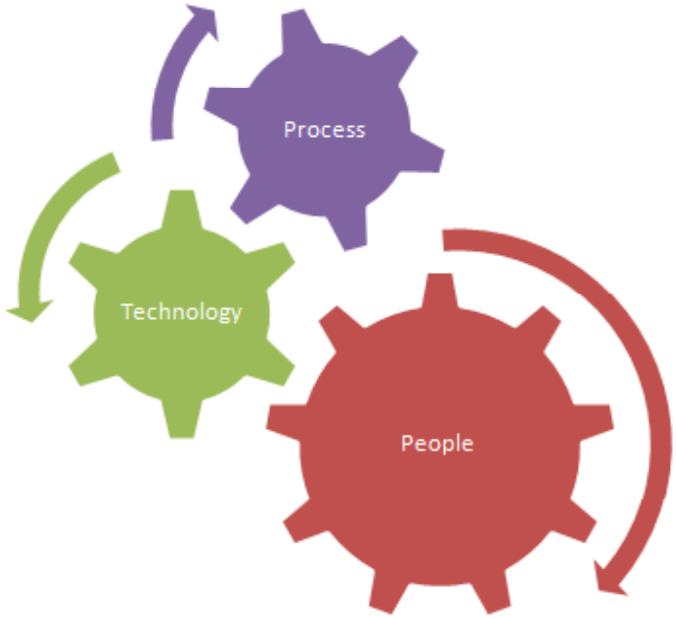
- Good processes
- Checks and balances
- Controls built in

People

- Background Checks
- Educated and aware
- Unified objectives

Technology

- People using good process with technology
- Compliance and Security validated



Assets

- Vendor Support
  - Infrastructure
  - Applications
  - Integration

Environments

- Baseline – Vendor
- Development
- Test
- Production

- **Incentives are needed to help**
  - **Vendors included in knowledge and funded**
  - **Industry needs funding for none traditional costs**

Solutions

- Architecture includes
  - Security
  - Compliance
- Working Solutions
  - Define strong mitigation(s)

- Improve INL SCADA Test Bed with more funding, vendors and support
- Fund ICCP solutions to fix vulnerabilities
- Education

Example: Information Protection

- **Challenges**
  - Modernization of facilities under NERC CIP required process enhancements and new processes
  - Getting buy-in and support
  - Practices with local and state government reviewed, examined, negotiated and implemented
- **Solutions**
  - Team Approach:

    Executives, Facility, Project Management, Legal, Security, Records Management and Compliance
  - Process Developed
    - Education and awareness
    - Contracts and agreements
      - Agreement for Proposal Services
      - Master Agreements
      - Non Disclosure Agreements
- **Education**

Resource:

Energy Sector Information Sharing and Analysis Center

- **Overview:** The ES-ISAC serves the Electricity Sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures**.**
- **Link:** **http://www.esisac.com/Default.htm**
  - ***To report any incidents related to this alert, contact:***
    - **ES-ISAC 24-hour hotline**
    - **609.452.1422**
    - **esisac@nerc.com**
- **Incident Response Planning:**
  - ***http://www.esisac.com/publicdocs/Guides/11a-Incident-Response.pdf***

Resource:

US-CERT Emergency Readiness Team

- **Overview:** Resource on cyber alerts and vulnerabilities.
  - ***Link:*** ***http://www.us-cert.gov/***
- **Incident Reporting**: How to report an incident and form.
  - ***Link:*** ***https://forms.us-cert.gov/report/***
- US-CERT Secured Portal: **Official use only portal. This system will allow all contractors of the system to collaborate with one another and with the government in a secure mode.**
  - ***Link:*** ***https://portal.us-cert.gov/***
- Vulnerability Reporting: **To submit a vulnerability under the secured portal:**
  - ***Link: https://portal.us-cert.gov/member/mail3/index.cfm?action=composeMessage&mailToPid=844&msgsubject=Reporting%20a%20Vulnerability***
- ICS-CERT - Industrial Control Systems Cyber Emergency Response Team:
  - ***Overview: The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to: Respond to and analyze control systems related incidents; Conduct vulnerability and malware analysis; Provide onsite support for incident response and forensic analysis; Provide situational awareness in the form of actionable intelligence. Coordinate the responsible disclosure of vulnerabilities/mitigations; Share and coordinate vulnerability information and threat analysis through information products and alerts***
  - ***Link:*** ***http://www.us-cert.gov/control_systems/ics-cert/***

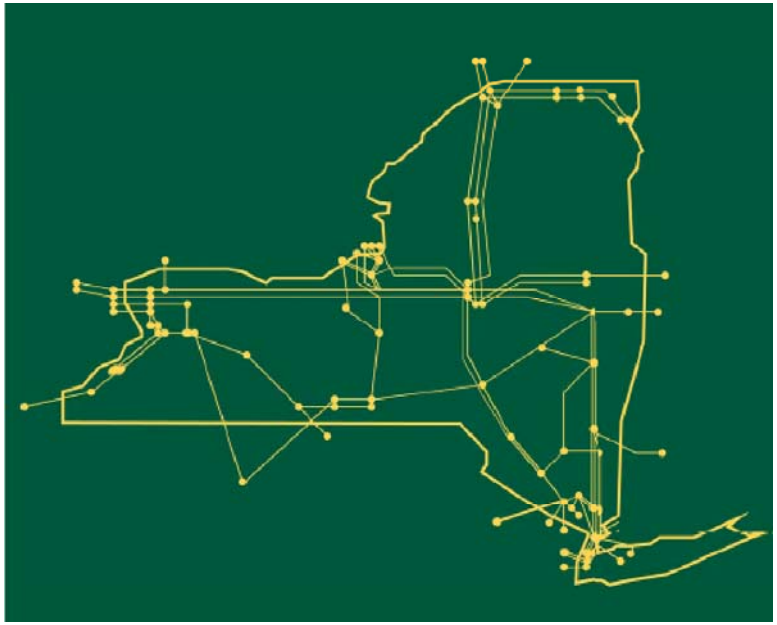
Resources: Vulnerabilities

- NIST National Vulnerability Database
  - *Overview:* ***This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.***
  - ***Link: http://nvd.nist.gov/***
- US-CERT Vulnerability Notes Database
  - *Overview:* ***US-CERT publishes information about a wide variety of vulnerabilities. Vulnerabilities that meet a certain severity threshold are described in US-CERT Technical Alerts***
  - ***Link: http://www.kb.cert.org/vuls***
- Vendors

Resources:

- DHS Daily Open Source Infrastructure Report
  - ***Link: http://www.dhs.gov/files/programs/editorial_0542.shtm***
- Department of Homeland Security - Homeland Security Information Network
  - ***Link: http://www.dhs.gov/files/programs/gc_1156888108137.shtm***
- United States Department Of State Bureau Of Diplomatic Security
  - ***Link: http://www.dhs.gov/files/programs/gc_1156888108137.shtm***
- New York Police Department Shield
  - ***Link: http://www.nypdshield.org/public/***
- Other Sources:
  - ***Slashdot - http://slashdot.org/***
  - ***Threatpost - http://threatpost.com/***
  - ***DarkReading - http://www.darkreading.com/***

The New York Independent System Operator (NYISO) is a not-for-profit corporation responsible for operating the state's bulk electricity grid, administering New York's competitive wholesale electricity markets, conducting comprehensive long-term planning for the state's electric power system, and advancing the technological infrastructure of the electric system serving the Empire State.



www.nyiso.com