COMPASS FOR THE COMPLIANCE WORLD
Asia Pacific ICS Security Summit
3 December 2013
**THE JOURNEY**

- Why are you going - **Mission**
- Where are you going - **Goals**
- How will you get there – **Reg. Stnd. Process**
- How will you know you are there - **Measure**
WHY ARE YOU GOING - MISSION

- Safety
- Reliability
- Critical Infrastructure Protection

Choice vs. Regulation

- Frameworks
  - ISA / IEC
  - NIST
  - ISO
<table>
<thead>
<tr>
<th>General</th>
<th>Policies &amp; Procedures</th>
<th>System</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 62443-1-1 Terminology, concepts, and models</td>
<td>• 62443-2-1 Requirements for an IACS security management system</td>
<td>• 62443-3-1 Security technologies for IACS</td>
<td>• 62443-4-1 Product development requirements</td>
</tr>
<tr>
<td>• 62443-1-2 Master glossary of terms and abbreviations</td>
<td>• 62443-2-2 Implementation guidance for an IACS security management system</td>
<td>• 62443-3-2 Security levels for zones and conduits</td>
<td>• 62443-4-2 Technical security requirements for IACS components</td>
</tr>
<tr>
<td>• 62443-1-3 System security compliance metrics</td>
<td>• 62443-2-3 Patch management in the IACS environment</td>
<td>• 62443-3-3 System security requirements and security levels</td>
<td></td>
</tr>
<tr>
<td>• 62443-1-4 IACS security lifecycle and use-cases</td>
<td>• 62443-2-4 Installation and maintenance requirements for IACS supplier</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Recommendations of the National Institute of Standards and Technology
NIST

- 800-82 reference
  - 800-53 with mod
  - 800-41 firewalls
  - 800-12 security policies
  - 800-26 security control assessments
  - 800-37 security certification
  - 800-18 preparing rules of behavior
  - 800-30 risk management
  - 800-39 risk assessments
  - 800-40 patching
  - 800-115 network security testing
  - 800-60 information security categories
NIST

- 800-82 reference
  - 800-23 acquisition and use
  - 800-27 engineering principles
  - 800-35 security services
  - 800-36 security product selection
  - 800-64 system development lifecycle
  - 800-65 capital planning and investment
  - 800-70 configuration settings
  - 800-73 interface for identity verification
  - 800-76 biometrics
  - 800-46 telecommuting and broadband
  - 800-34 contingency planning
NIST

- 800-82 reference
  - 800-63 authentication for remote maintenance
  - 800-94 IDS IPS
  - 800-88 equipment sanitization
  - 800-61 incident handling
  - 800-83 incident prevention
  - 800-16 security training
  - 800-50 security awareness
  - 800-77 VPN
  - 800-97 802.11i wireless security
  - 800-78 cryptography
  - 800-92 log management
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

Published standards  [edit]

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
- ISO/IEC 27001 — Information security management systems — Requirements. The older ISO/IEC 27001:2005 standard relied on the Plan-Do-Check-Act cycle; the newer ISO/IEC 27001:2013 does not, but has been updated in other ways to reflect changes in technologies and in how organisations manage information.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)
- ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)
- ISO/IEC 27010 — Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 — Information security governance
- ISO/IEC TR 27015 — Information security management guidelines for financial services
- ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27032 — Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 — Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27034 — Guideline for application security
- ISO/IEC 27035 — Security incident management
- ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and presentation of digital evidence
- ISO 27799 — Information security management in health using ISO/IEC 27002
DO SOMETHING!

- Benchmark
- Use Existing Standards
- Do Not Start Over
- Do Not Use Corporate Policies
WHY ARE YOU GOING - MISSION

- Safety
- Reliability
- Critical Infrastructure Protection

Events = Corrective Action

- Regulatory Compliance
EVENT = ACTION

Alert: Major cyber attack aimed at national gas

Aramco Says Cyberattack Was Aimed at Production

By REUTERS
Published: December 29, 2013

JEJDAH, Saudi Arabia (Reuters) - Saudi Aramco, the world's largest oil company, Aramco, said on Friday it had detected a "major" cyber attack aimed at its oil and gas production facilities in the Middle East.

The attack on Saudi Arabia's oil - a failure to oil - oil relatively rare hacking strikes in the oil industry.

"The main target was to disrupt local and international facilities and achieve their goals," Aramco chief executive Amin Nasser said in a statement.

Nasser said the company had taken measures to prevent further damage.

"We will not tolerate such acts," he said. 

Aramco, which supplies 20% of global demand, said it had worked with the Saudi cyber security taskforce to block the attackers.

The company said it had no details on how the attack was carried out or who was behind it.

Aramco, which is listed on the London Stock Exchange, has 30% of the world's known oil reserves.

By Mark Collins

DHS: Spear Phishing Campaign Targeted 11 Energy Firms

BERLIN, Germany (Reuters) - German security researchers warned on Saturday of a spear-phishing campaign targeting 11 energy firms in the U.S., following similar attacks on the Department of Labor.

A spear phishing campaign is when an attacker sends a malicious email to a specific target, often with the aim of harvesting sensitive information.

The Department of Labor said last month that its website had been hacked, but did not specify what kind of attack it was.

The attacker used a variety of techniques, including phishing, to try to trick employees into clicking on links that would install malware.

"The hackers were very sophisticated," said one of the researchers.

"They were able to use social engineering techniques to find our employees' email addresses and then send them fake emails that appeared to come from companies they worked for.

"Once the employees clicked on the links, the malware would be installed on their computers, giving the hackers access to their email accounts and other sensitive information.

"This is a very serious threat. We need to be more aware of these kinds of attacks and take steps to protect ourselves.

The researchers said they had found evidence that the attackers were also targeting other sectors, including government organizations.

Oil, Energy Watering hole Attacks Could Be Tied to DDoS Attacks

WASHINGTON, June 17, 2013 (Reuters) - A string of watering hole attacks targeting oil and energy companies dating back to May could be linked to similar attacks against the U.S. Department of Labor website.

"These attacks are very sophisticated, and we need to be aware of them," said one of the researchers.

"We need to work with the companies affected to find out how their networks were compromised.

"Once we have that information, we can take steps to protect ourselves and our customers.

The researchers said they had found evidence that the attackers were using a variety of techniques, including social engineering, to try to gain access to the companies' networks.

"They were using phishers to gather information about our employees and then use that information to try to trick them into clicking on links that would install malware.

"The attackers were also using malware to try to exploit vulnerabilities in our systems.

"This is a very serious threat, and we need to take steps to protect ourselves and our customers.

The researchers said they were working with the companies affected to find out how their networks were compromised and to take steps to protect themselves and their customers.

OIL, ENERGY WATERING HOLE ATTACKS COULD BE TIED TO DDoS ATTACKS

by Michael Mimoso

Follow @mike_mimoso

September 19, 2013, 3:55 pm

A string of watering hole attacks targeting oil and energy companies dating back to May could be linked to similar attacks against the U.S. Department of Labor website.

"These attacks are very sophisticated, and we need to be aware of them," said one of the researchers.

"We need to work with the companies affected to find out how their networks were compromised.

"Once we have that information, we can take steps to protect ourselves and our customers.

The researchers said they had found evidence that the attackers were using a variety of techniques, including social engineering, to try to gain access to the companies' networks.

"They were using phishers to gather information about our employees and then use that information to try to trick them into clicking on links that would install malware.

"The attackers were also using malware to try to exploit vulnerabilities in our systems.

"This is a very serious threat, and we need to take steps to protect ourselves and our customers.

The researchers said they were working with the companies affected to find out how their networks were compromised and to take steps to protect themselves and their customers.

OIL, ENERGY WATERING HOLE ATTACKS COULD BE TIED TO DDoS ATTACKS

by Michael Mimoso

Follow @mike_mimoso

September 19, 2013, 3:55 pm

A string of watering hole attacks targeting oil and energy companies dating back to May could be linked to similar attacks against the U.S. Department of Labor website.

"These attacks are very sophisticated, and we need to be aware of them," said one of the researchers.

"We need to work with the companies affected to find out how their networks were compromised.

"Once we have that information, we can take steps to protect ourselves and our customers.

The researchers said they had found evidence that the attackers were using a variety of techniques, including social engineering, to try to gain access to the companies' networks.

"They were using phishers to gather information about our employees and then use that information to try to trick them into clicking on links that would install malware.

"The attackers were also using malware to try to exploit vulnerabilities in our systems.

"This is a very serious threat, and we need to take steps to protect ourselves and our customers.

The researchers said they were working with the companies affected to find out how their networks were compromised and to take steps to protect themselves and their customers.
Keynote:
Economic Impacts
Political Impacts
Operational Impacts
Emotional Impacts

Response:
1. Enhance Security Resiliency
2. Promote Security Awareness
3. Workforce Development
NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAMS

http://www.cert.org/csirts/national/contact.html
Events = Action

First half of fiscal year 2013 ICS-CERT has responded to over 200 incidents across all critical infrastructure sectors, with the highest percentage of incidents reported occurring in the energy sector at 53%.
EVENT = ACTION

February 12, 2013 – Executive Order 13636
Improving Critical Infrastructure Cybersecurity

Defines critical infrastructure -

to mean systems and assets, whether **physical or virtual**, so vital to the United States that the incapacity or destruction of such **systems and assets would have a debilitating impact** on security, national economic security, national public health or safety, or any combination of those matters 42 U.S.C. 5195c(e).
NIST STANDARDS PURSUANT TO EO

“NIST will create a cyber security framework.”

NIST Framework -- five functions and detailed Appendices:

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Draft Released – August 28, 2013
October 10 -- Preliminary Cybersecurity Framework
Scheduled for February, 2014 -- Final release*
THE EXECUTIVE ORDER (EO)

- “This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.”

- Core goal is voluntary sharing
5:28 P.M., NOV. 9th
THE LIGHTS WENT OUT

= North American Electric Reliability Council

11/9/1965
8/14/2003

= North American Electric Reliability Corporation
CHECKPOINT #1

- Mission Focused action and Standards adoption is admirable and should be pursued
- Voluntary and Incentive driven Standards Frameworks will eventually shape mandatory regulations
- Events in your sector or region will result in Mandatory Compliance
WHERE ARE YOU GOING?

- Regulation
  - Security in Regulation
  - Sector Specific
    - NRC NEI
    - NERC CIP,
## How Security Fits with Regulations

### Engineering and Designing Cyber Solutions
- Engineering services to design secure, operationally viable and efficient systems, including:
  - Security Requirements Analysis & Development
  - Infrastructure Requirements Analysis & Development
  - Secure Network Design
  - Secure Applications Design
  - Data Center Design
  - Server Design
  - Storage Design
  - End User Solutions Design
  - System Security Engineering
  - Enterprise Security Architecture
  - Infrastructure Architecture
  - Information Systems Security Engineering

### Operating Cyber Solutions
- Planning, Operations and Monitoring Services to execute full spectrum cyber operations, including:
  - Cyber Policies, Plans, & Procedures Services
  - IT Asset Management Services
  - Cyber Operation Planning and Execution Services
  - Intrusion Detection & Prevention
  - Incident Response/Problem Management Services
  - Secure Systems Monitoring
  - Security Performance Measurement and Monitoring
  - COMSEC Monitoring
  - Blue/Red Teaming Services
  - Secure Supply Chain
## How Security Fits with Regulations

### Assessing Cyber Solutions –
Diagnostic services to assess the security, operational viability and efficiency of systems, including

<table>
<thead>
<tr>
<th>Forensic Analysis</th>
<th>Penetration Testing</th>
<th>Security Testing</th>
<th>Common Criteria Testing</th>
<th>Infrastructure Assessment</th>
<th>Supply Chain Security Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Managing IT/Network Services –
IT and Network Management services to operate secure and efficient networks and systems, including

<table>
<thead>
<tr>
<th>Service Center/Call Center Services</th>
<th>Secure Systems Administration Services</th>
<th>Secure Systems Configuration Management Services</th>
<th>ITIL Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Security Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations Services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Managing, Building and Implementing Cyber Solutions**

<table>
<thead>
<tr>
<th>Wired Network Solutions</th>
<th>Emergency Communications</th>
<th>Virtualization Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid Networking Solutions</td>
<td>Cross Domain Solutions</td>
<td>Data Center Solutions</td>
</tr>
<tr>
<td>Wireless Technologies and Mobile Computing Solutions</td>
<td>Public Key Infrastructure Solutions</td>
<td>Server Solutions</td>
</tr>
<tr>
<td>Mobile &amp; Wireless Security Solutions</td>
<td>Identity &amp; Access Management Solutions</td>
<td>Storage Solutions</td>
</tr>
<tr>
<td>COMSEC/Cryptographic Solutions</td>
<td>Cyber Exploitation Solutions</td>
<td>End User Solutions</td>
</tr>
<tr>
<td>Unified Communications Solutions</td>
<td>Cloud Computing Solutions</td>
<td>IT Disaster Preparedness &amp; Recovery Solutions</td>
</tr>
<tr>
<td></td>
<td>Infrastructure as a Service Solutions (IaaS)</td>
<td>Secure Supply Chain Solutions</td>
</tr>
</tbody>
</table>
SCOPE OF REGULATORY IMPACT

**Assets**
- Physical Protection
- Electronic Protection
- Asset Management

**Information**
- Physical Protection
- Electronic Protection
- Data at Rest and In Motion

**People**
- Qualifications for access (PRA / Training)
- Access Control
- Least Privilege
HOW WILL YOU GET THERE - EXAMPLE REGULATION

- NRC / NEI (Nuclear Regulatory Commission / Nuclear Energy Institute)
  - Staggered implementation schedule
- NERC CIP (Critical Infrastructure Protection)
  - Years of implementation – mature enforcement
Integration and Risk Mitigation

Instrumentation and Controls, including CDA

Cyber and Physical Security

Supply Chain Security and Optimization

Program Management, Training and Documentation

Regulations Standards and Policy Compliance

Incident Response and Emergency Preparedness
NUCLEAR SECTOR REGULATION EXAMPLE

- NRC - Title 10 of the Code of Federal Regulation (CFR)
  - 10 CFR 73.54 - Protection of digital computer and communication systems and networks.
  - RG 5.71 – The Regulatory Guide for the Rule
  - Scope of Systems now includes balance of plant
  - SSEP Security, Safety, Emergency Preparedness and support systems
# Key Regulatory Cyber Security Requirements

<table>
<thead>
<tr>
<th>Establish a Cyber Security Plan (CSP)</th>
<th>Identify Critical Data Assets (CDA)</th>
<th>Align CSP and Physical Security Plan/Program</th>
<th>Implement Supply Chain Protections</th>
<th>Conduct Training and Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. NRC 5.71</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NEI 08-09</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>U.S. § 73 &amp; 73.54</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

## Nuclear Cyber Security Regulation Requirements

<table>
<thead>
<tr>
<th>Regulation</th>
<th>List of Requirements</th>
</tr>
</thead>
</table>
| **U.S. NRC 5.71**| - As stated in 10 CFR 73.54(e), the licensee must establish, implement, and maintain a cyber security plan that satisfies the cyber security program requirements of this regulation.  
  - A licensee must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs, which are those assets that, if compromised, could adversely impact the SSEP functions of nuclear facilities.  
  - Identify ALL Critical Digital Assets within the site.  
  - A licensee must incorporate the cyber security program into its physical protection program.  
  - Licensee/Applicant protects against supply chain threats and vulnerability.                                                                                                                                  |
| **NEI 08-09**    | - Establish, implement, and maintain a cyber security program for the protection of the assets  
  - Analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber attacks  
  - The licensee shall protect the systems and networks from cyber attacks that would adversely impact the operation of systems, networks, and associated equipment.  
  - Incorporate the cyber security program as a component of the physical protection program  
  - The licensee shall protect digital computer and communication systems and networks                                                                                                                                 |
| **U.S. § 73 & 73.54** | - Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a)  
  - Perform site analysis of all digital computer and communications systems and networks  
  - Evaluate ALL modifications to CDAs prior to implementation to achieve high assurance that digital computer and communications systems and networks are adequately protected against cyber attacks  
  - Incorporate the cyber security program into the physical security protection program  
  - The site shall establish a formal, documented, system and services acquisition policy                                                                                                                                 |
CURRENT STATUS

- Site specific implementation dates (approved)
- Cyber Security programs
- Policies, procedures, measures
- Training
- Inspection program in development and pilot
OVERVIEW OF NERC COMPLIANCE

MOD
- Modeling, Data & Analysis
  - 22 standards
  - 89 Requirements
  - 210 Sub Req

PEO
- Personnel, Performance & Qualifications
  - 5 standards
  - 11 Requirements
  - 15 Sub Req

PRO
- Protection & Control
  - 22 standards
  - 73 Requirements

TPP
- Transmission Protection
  - 9 standards
  - 47 Requirements
  - 119 Sub Req

TOP
- Transmission Operations
  - 8 standards
  - 55 Requirements
  - 17 Sub Req

EOP
- Emergency Operations
  - 9 standards
  - 68 Requirements
  - 146 Sub Req

FAC
- Facility Connection & Maintenance
  - 10 standards
  - 36 Requirements
  - 270 Sub Req

INT
- Interconnection Reliability Operations
  - 12 standards
  - 53 Requirements
  - 35 Sub Req

CIP
- Critical Infrastructure Protection
  - 9 standards
  - 47 Requirements
  - 119 Sub Req

BAL
- Resource & Demand Balancing
  - 6 standards
  - 41 Requirements
  - 35 Sub Req

COM
- Communications & Coordination
  - 2 standards
  - 8 Requirements
  - 5 Sub Req

* Values obtained vary based on entity functional registration
OVERVIEW OF NERC COMPLIANCE

* Values obtained vary based on entity functional registration
**How will you know when you get there - Measure**

- Self Assessments
- Peer Assessments
- Inspections with recommendations
- Audits with enforcement actions
7 of the top 10 most violated standards are CIP
**ENFORCEMENT**

* Largest penalty to date – 25M FPL for 2008 blackout that impacted millions of customers for several hours

<table>
<thead>
<tr>
<th>Violation Risk Factor</th>
<th>Lower</th>
<th>Moderate</th>
<th>High</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Range Limits</td>
<td>Range Limits</td>
<td>Range Limits</td>
<td>Range Limits</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Lower</td>
<td>$1,000</td>
<td>$3,000</td>
<td>$2,000</td>
<td>$7,500</td>
</tr>
<tr>
<td>Medium</td>
<td>$2,000</td>
<td>$30,000</td>
<td>$4,000</td>
<td>$100,000</td>
</tr>
<tr>
<td>High</td>
<td>$4,000</td>
<td>$125,000</td>
<td>$8,000</td>
<td>$300,000</td>
</tr>
</tbody>
</table>
### Demonstrated Penalties

<table>
<thead>
<tr>
<th></th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Fines issued</td>
<td>-218</td>
<td>Total Fines issued - 258</td>
</tr>
<tr>
<td>Average fine</td>
<td>9,381</td>
<td>Average fine – 21,764</td>
</tr>
<tr>
<td>Total Fine</td>
<td>2,026,400</td>
<td>Total Fine – 5,615,100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Fines issued</td>
<td>-394</td>
<td>Total Fines issued - 252</td>
</tr>
<tr>
<td>Average fine</td>
<td>24,057</td>
<td>Average fine – 37,048</td>
</tr>
<tr>
<td>Total Fine</td>
<td>9,310,193</td>
<td>Total Fine – 9,262,097</td>
</tr>
</tbody>
</table>

*Values obtained from NOV data at NERC website, values are approximate*
# of penalties

- Chart showing the number of penalties with a peak in 2011.

average penalty

- Chart showing the average penalty increasing over the years.

total penalty

- Chart showing the total penalty increasing over the years.
REGULATORY CHANGE AND LAG
DYNAMIC ENVIRONMENT

2004 - 2005
Urgent Action Standard 1200

2006 - 2009
CIP002 – CIP009 version 1

2010 April
CIP002 – CIP009 version 2

2010 October
CIP002 – CIP009 version 3

2011 Approved – Skip Implementation
CIP002 – CIP009 version 4

2013 approved November – Implementation 2015
CIP002 – CIP011 version 5
Risk-Based Assessment must consider the seven items detailed in: CIP002-R1.2 Sub-Requirements: R1.2.1-R1.2.7
Risk Based Assessment Methodology

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator’s restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator’s restoration plan.

1.11. Each Transmission Requirement.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.
2.3. Each generation Facility that its Planning Coordinator designates, and informs the Generator Coordinator, may avoid an Adverse Reliability Impact in the following situations:

2.4. Transmission Facilities operated at 500 kV or above in the collector bus for a generation plant, are not parts of the generation interconnection Facility.

2.5. Transmission Facilities that are operating in a station or substation, where the station voltages to three or more other Transmission Facilities “aggregate weighted value” exceeding 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

2.6. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Coordinator, or Transmission Planner and Operator for an aggregate high reliability system, used to perform the functional obligations of the Transmission Operator for any of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

2.7. Each Control Center used to perform the functional obligations of the Reliability Coordinator for any of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2.8. Each Control Center used to perform the functional obligations of the Generator Operator for any of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2.9. Each Special Protection System (SPS), that if destroyed, degraded, or otherwise rendered unavailable, would result in the loss of the generation of a facility, the operation of the System, or as a result of its application to the Transmission Facility.

2.10. Each system or group of Elements that are a common control system, with a Planning Coordinator, is implementing undervoltage load shedding (UVLS) under load shedding limits as a NERC or regional reliability system.

2.11. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for an aggregate high reliability system, used to perform the functional obligations of the Transmission Operator for any of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for any of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2.13. Each Control Center used to perform the functional obligations of the Transmission Operator for any of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

3. Low Impact Rating (L)

BES Cyber Systems not included in Section 1 above, associated with any of the following assets and that meet the applicable requirements:

3.1. Control Centers and backup Control Centers, used to perform the functional obligations of the Generator Coordinator, or Transmission Planner and Operator for any of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

3.2. Transmission lines and substations, that meet criterion 2.1, 2.3, 2.6, or 2.9.

3.3. Generation resources.

3.4. Systems and facilities critical to the System, with a Planning Coordinator, or Transmission Planner and Operator for any of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

3.5. Special Protection Systems that have a Planning Coordinator, or Transmission Planner and Operator for any of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

3.6. For Distribution Providers, Providers, and their Subcontractors, that meet criterion 2.1, 2.3, 2.6, or 2.9.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority for generation equal or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that is aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

Voltage Value of a Line

<table>
<thead>
<tr>
<th>Voltage Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 200 kV</td>
<td>(not applicable)</td>
</tr>
<tr>
<td>200 kV to 299 kV</td>
<td></td>
</tr>
<tr>
<td>300 kV to 499 kV</td>
<td></td>
</tr>
<tr>
<td>500 kV and above</td>
<td></td>
</tr>
</tbody>
</table>
CHECKPOINT # 2

- Security requirements will be in the regulation and they will lag vulnerabilities, and technology
- The requirements will not work on many ICS devices - one size does not fit all
- Focus will be on documentation and audit evidence production
- Significant systems will need to be implemented to ensure compliance
- Consider misuse not just availability of assets
- Work very closely with your vendors
**Final Thoughts**

- Process is unpredictable and poorly controlled
- Managed
- Defined
- Quantitatively Managed
- Process is proactive typically driven by the “organization”
- Process is measured and controlled
- Scorecards and metrics
- Integrating into asset management
- Integrating into procurement
- Select a framework or standard
- Benchmarking and community efforts
- Continuous process improvement
- Optimizing

- Scorecards and metrics
- Integrating into asset management
- Integrating into procurement
- Select a framework or standard
- Benchmarking and community efforts
- Continuous process improvement
- Optimizing
**FINAL THOUGHTS**

- **Implementation plan**
  - Initial: Process is unpredictable and poorly controlled
  - Managed: Process is reactive typically driven by “projects”
  - Defined: Process is proactive typically driven by the “organization”
  - Optimizing: Continuous process improvement

- **Achieving Compliance projects**
- **Managing Compliance process**
- **Enforcement audits**
  - Industry performance assessments

- **Managing Compliance process**
  - Quantitatively Managed
  - Process is measured and controlled

- **Optimizing**

LAST CHECKPOINT

- If you have no regulation currently, take action before action is taken for you
- Ensure leadership understands compliance does not equal security
- Ensure balanced investment in both compliance and security
- Do not fear the auditor more than the attacker
tconway@sans.org