WELCOME TO MEETING #3 – PEOPLE / PROCESS

WORKING GROUP 3 (RELIABILITY, RESILIENCY, AND CYBER SECURITY)
<table>
<thead>
<tr>
<th>Time</th>
<th>Agenda Item</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00AM – 9:10AM (10 minutes)</td>
<td>Meeting #2 Recap, Other Updates</td>
<td>WG3 Co-Leads</td>
</tr>
<tr>
<td>9:10AM – 10:10AM (60 minutes)</td>
<td>People / Process Presentations</td>
<td>NERC, EPRI, Ameren</td>
</tr>
<tr>
<td>10:10AM – 11:00 AM (50 minutes)</td>
<td>People Discussion</td>
<td>WG Members, WG Co-Leads</td>
</tr>
<tr>
<td>11:00AM – 11:05AM (5 minutes)</td>
<td>BREAK</td>
<td></td>
</tr>
<tr>
<td>11:05AM – 11:55 AM (50 minutes)</td>
<td>Process Discussion</td>
<td>WG Members, WG Co-Leads</td>
</tr>
<tr>
<td>11:55AM – 12:00PM (5 minutes)</td>
<td>Questions? Process Discussion Items to Carryover to Next Meeting? Next Steps &amp; Call for Presenters</td>
<td>WG Co-Leads</td>
</tr>
</tbody>
</table>
WORKING GROUP RECAP, AND OTHER UPDATES

CO-LEADS:
MANIMARAN GOVINDARASU
DOMINIC SAEBELEER
RELIABILITY: “ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components”

SECURITY: “ability of a system or its components to withstand attacks (including physical and cyber incidents) on its integrity and operations”

RESILIENCY: “ability of a system or its components to adapt to changing conditions and withstand and rapidly recover from disruptions”

Definitions from DOE Quadrennial Energy Review: Second Installment: Chapter IV)
PROPOSED APPROACH
Technology, People, Process, and Regulation
SMART GRID: A CYBER-PHYSICAL SYSTEM

Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, Reliability Standards, February 2012
Figure 2: High-performing compliance organizations focus on four key elements

- **Role of compliance**
  - Aligned with regulations, business strategy and enterprise risk appetite
  - Clear principles and metrics that support this role

- **Enablers: People, processes, systems**
  - Right leadership skills, with strong performance management
  - Effective, efficient end-to-end processes, enabled by technology
  - Activities delivered out of most effective, lowest-cost environment

- **World-class compliance program**

- **Policies, programs and priorities**
  - Risk-based policies and standards
  - Well-defined and prioritized activities

- **Cross-functional operating model**
  - Clear roles, decisions and accountabilities
  - Supporting structure and organization design
  - Governance, monitoring and oversight
  - Ways of working and a culture of doing the right thing

Source: Bain & Company
# Topics Matrices

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology</strong></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td><strong>Regulations &amp; Compliance</strong></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
<tr>
<td></td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
<td>&quot; &quot; &quot; &quot;</td>
</tr>
</tbody>
</table>

NextGrid Illinois
PEOPLE / PROCESS PRESENTATIONS
Electricity Information Sharing and Analysis Center

Bill Lawrence, Director of the E-ISAC
NextGrid Webinar
May 11, 2018
E-ISAC mission and vision
E-ISAC products and services
NextGrid process priority topics
  - Metrics (#3)
  - Harmonizing frameworks (#5)
  - Exercising (evaluation and testing) (#6)
E-ISAC points of contact
Mission

The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration.

Vision

To be a world class, trusted source for the quality analysis and rapid sharing of electricity industry security information.
### Products
- Subject matter experts for NERC Alerts
- Incident (cyber and physical) bulletins
- Weekly, monthly, and annual summary reports
- Issue-specific reports

### Programs and Services
- Monthly briefing series, first Tuesday of the month
- Grid Security Conference (GridSecCon)
- Grid Exercise (GridEx)
- Cyber Risk Information Sharing Program (CRISP)
- Industry Augmentation Program (IAP)

### Tools
- E-ISAC portal (www.eisac.com)
- Critical Broadcast Program (CBP) notifications
- Cyber Automated Information Sharing System (CAISS)
• 3. Address need for metrics to quantify effectiveness of interventions

   Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2)
Figure 3: Domains Graphical Summary of the C2M2 Survey
• We:
  ▪ Can learn from other domains
  ▪ Have more data than we think
  ▪ Need less data than we think
  ▪ Can make better security and investment decisions using quantitative, probabilistic methods
5. Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria

E-ISAC

- Portal with dedicated user communities [www.eisac.com](http://www.eisac.com)
  - Voluntary information sharing and required reporting
- Cyber Automated Information Sharing System (CAISS)
- Cyber Risk Information Sharing Program (CRISP)
- Cross-sector and federal government partners

Other opportunities

- DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- National Guard
- FBI field offices
- DHS Protective Security Advisors
6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities

- Department of Energy’s regional exercise initiatives
- National Exercise Program (NLE, Cyber Storm, etc.)
- NERC’s biennial GridEx IV
GridEx is an unclassified public/private exercise designed to simulate a coordinated cyber/physical attack with operational impacts on electric and other critical infrastructures across North America to improve security, resiliency and reliability.
• Exercise incident response plans
• Expand local and regional response
• Engage critical interdependencies
• Improve communication
• Gather lessons learned
• Engage senior leadership
**Exercise Components**

**Move 0**
**Pre-Exercise**

- **Preparation**
- **Identification**
- **Containment**

Operators may participate in Cyber Intrusion detection activities

**Distributed Play**
(2 days)

- **Utilities**
- **Reliability Coordinators**
- **Support and Vendors**
- **E-ISAC and BPSA**
- **Fed/State/Prov Agencies**

Players across the stakeholder landscape will participate from their local geographies

**Executive Tabletop**
(1/2 day)

Facilitated discussion engages senior decision makers in reviewing distributed play and exploring policy triggers

---

*RESILIENCY | RELIABILITY | SECURITY*
GridEx Participation

GridEx Exercise Participation

- GridEx 2011:
  - Active: 36 (47%)
  - Observing: 40 (53%)

- GridEx II:
  - Active: 122 (53%)
  - Observing: 109 (47%)

- GridEx III:
  - Active: 155 (57%)
  - Observing: 209 (43%)

- GridEx IV:
  - Active: 335 (74%)
  - Observing: 117 (26%)
GridEx IV: Who Participated?

- 6500 Participants
- 206 Electric utilities
- 450 Organizations
- 17 Cross-sector partners
- 10 States (2 full-scale)
• GridEx V is November 13-14, 2019
• GridSecCon 2018 in Las Vegas, NV, October 15-19
• E-ISAC points of contact
  - events@eisac.com
  - memberservices@eisac.com
  - operations@eisac.com
Questions and Answers
Illinois NextGrid: Utility of the Future Study

WG3: Reliability, Resiliency, and Cyber Security

Galen Rasche
Sr. Program Manager, Cyber Security
grasche@epri.com

May 11, 2018
About the Electric Power Research Institute

**Independent**
Objective, scientifically based results address reliability, efficiency, affordability, health, safety, and the environment

**Nonprofit**
Chartered to serve the public benefit

**Collaborative**
Bring together scientists, engineers, academic researchers, and industry experts
Industry Trends Impacting Cyber Security Risk

**Generation, Transmission & Distribution**
- Real-time situational awareness
- Dynamic supply / demand balancing with DER (DERMS)
- Mobile workforce
- Increased automation and communications

**Customer**
- Self generation (Solar PV, Storage,..)
- Electric vehicles
- IoT devices

**Third Parties**
- DER and DR aggregators

**National Security/Resiliency Mindset**
- Malicious attack or natural catastrophe
Information, Communication and Cyber Security Roadmap

EPRI’s Cyber Security Program R&D for Industry…

- **Mitigate risks** to legacy and next-generation grid systems
- **Improve security** with advanced network and threat management technology and practices
- **Effectively evaluate** security program processes
- **Learn** how peer utilities address their security challenges
- **Leverage** EPRI’s industry expertise, sector knowledge, and Cyber Security Research Lab to provide value ranging from thought leadership to hands-on demonstrations
IT/OT Security Convergence

Incident Response
• Integrated Security Operations Center
• IDS/IPS
• Forensics
• Security Data Analytics

Situational Awareness
• Developing near-real-time knowledge of a dynamic operating environment
• Common Operating Picture

Threat Management
• OT threat intelligence use cases, methodologies, and tools

Asset and Configuration Management
• Technologies to improve device identification and configuration management
12:58 & 1:07 a.m. AT&T fiber-optic telecommunications cables were cut and Internet Service Provider network cables cut near Metcalf substation

1:31 a.m. Surveillance camera at substation recorded a streak of light followed by muzzle flash of rifles and sparks from bullets hitting the fence.

1:37 a.m. PG&E received an alarm from motion sensors at the substation, possibly from bullets grazing the fence.

1:41 a.m. Sheriff’s department received a 911 call about gunfire.

1:45 a.m. The transformers, riddled with bullet holes leaked 52,000 gallons of oil, overheated, PG&E’s control center received equipment-failure alarm.

1:51 a.m. Police officers arrived, but found everything quiet. Unable to get past the locked fence and seeing nothing suspicious, they left.

3:15 a.m. A PG&E worker arrived to survey the damage

* https://en.wikipedia.org/wiki/Metcalf_sniper_attack

How quickly can utilities correlate these events with Siloed Monitoring and Analysis?
Integrated Security Operations Center (ISOC)

- **IT Security Events**
  - Network Device Logs
  - IT System Logs
  - Business Systems

- **Physical Security Systems**

- **Threat and Vulnerability Information Sources**

- **Behavioral Learning Appliances**

- **Industrial Security Appliances**

- **OT Security Events**
  - Control Center Systems
  - Substation Gateways
  - Field Devices

- **Grid Operations Events**

- **Field Network Operations Center**

- **Log and Event Aggregation**

- **Correlation Engine**

- **Reporting**

Security Information and Event Management (SIEM)
What Are Security Metrics?

Numbers representing the **EFFECTIVENESS** of security controls
Security Metrics – Where does it fit?

- Framework for creating and implementing cybersecurity program
- Measuring the maturity of cybersecurity programs
- Measuring effectiveness of cybersecurity program
- Mandatory or discretionary requirements for the program

NIST Cybersecurity Framework
NERC CIP, NIST SP 800 53, NISTIR 7628
C2M2
Security Metrics
Why Do We Need Security Metrics?

Security Team
- To find out what works and what does not work
- To communicate security posture, threats, and risks
- To demonstrate value of their work

IT/OT Management
- Make sound decisions on security technology, resource allocation, etc.
- To trend the effectiveness of security controls over time
- Make recommendations to senior management on security priorities

Senior Management / The Board
- Assess the cyber security risk
- Make strategic decisions on cyber security risk management

Stakeholders
- “Is our data secure?”
- “Is our power grid secure?”
Recap: EPRI’s Security Metrics

3 Strategic Metrics
- Protection Score
- Detection Score
- Response Score

10 Tactical Metrics
- Network Perimeter Protection Score
- Threat Detection Score
- End-Point Protection Score
- ...

46 Operational Metrics
- Mean Time To Containment
- Monthly Count of Incidents involving Malicious Email
- Security Event True Positive Rate
- ...
- CVSS of a vulnerability
- Number of internal IPs reachable from an asset
- Database criticality rating
- ...

120~ Data Points
Cyber Security Challenges for the Multi-Party Grid

- Generation and storage assets may not be owned or operated by the utility
- Energy generation/consumption can be controlled by an aggregator
- Technology and business services are performed by third parties
- Operating increasingly complex, interconnected systems
- Dynamic governance relationships

How should the industry address these challenges?
The Path Forward

- Multi-Party Grid Risk Model
- Framework for Collaborative Security Management
- Cyber Security Guidelines for DER Integration
- Light-weight Encryption
- Simple Certificate or Cryptographic Key Management Scheme
- Cloud Security for Cyber-Physical Systems
Together…Shaping the Future of Electricity
The Human Factor: Challenges and Opportunities

NextGrid WG3 | 05.11.2018

Eric Herr | Director Cybersecurity Operations
Institutionalizing Cybersecurity

Current State
- Mandatory training
- Simulations
- Functional scorecards
- Awareness campaigns

Opportunities
- Gamification - make training fun
- Incentivize secure behaviors
- Include cybersecurity curriculum in all degree programs
- Partner with the trades to develop competencies in apprenticeship programs
Developing a Security Mindset

Current State

• Organizational boundaries exist between IT and OT
• Heavy reliance on network segmentation for security
• Different security technologies in IT and OT operated by different teams
• Situational awareness gaps

Opportunities

• Integrate IT/OT operations
• Reduce technical debt
• Align roles and responsibility by competency
• Develop the hunting discipline
• Career rotations within government and industry agencies
## Threat Intelligence and Adversary Behavior

### Current State
- Labor intensive process
- Heavy focus on static indicators of compromise
- Little orchestration of threat data across technology
- Lack of security clearance prohibits access to timely threat intelligence data

### Opportunities
- Threat and vulnerability is primed for automation and RPA use cases
- Analysts focus on adversary tradecraft, not static indicators
- Lobby to reduce dwell time on clearances
- Expand programs such as DOE CRISP and others to all utilities
Educating the Customer

Current State

• Little direct communication to customers regarding security of IoT devices

• Consumer IoT device configurations are not secure out of the box and updates can be complicated

Opportunities

• As an industry, we should educate consumers on risks associated with IoT devices

• Include cybersecurity curriculum in primary and secondary education

• Evolve the cybersecurity awareness campaign at the state level
Building a Cybersecurity Workforce

Opportunities

• Develop recruiting pipelines into universities and military
• Encourage and support a diverse cybersecurity workforce
• Support and participate with innovation hubs, hackathons, summer camps and other mentoring opportunities at all levels of education
• Create an exciting, dynamic workspace
• Incentivize professional growth
• Broaden adoption of cybersecurity scholarships
• Support apprenticeships as entry to cybersecurity careers
DISCUSSION FORMAT

**Purpose:** Describe challenge, identify opportunities, suggest solutions, and propose action items.

**Participant Feedback:** Let us know if this discussion format is not optimal

**WebEx Protocol:**
- Raise hand or send chat message to let host know you have a comment or question
- Host will notify who has the floor and who is on deck
WORKING GROUP
PEOPLE DISCUSSION
# PEOPLE OVERVIEW

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensuring a collaborative and consistent approach towards achieving a higher level of cyber and physical security</td>
<td>Building resiliency throughout ecosystem; growing employee skillset</td>
<td>Capability measurement: a. Baseline and advanced capabilities b. Drivers’ license type certification</td>
<td>Achieving a baseline level of cyber and physical security competency among all personnel</td>
<td>[input sought, if any]</td>
</tr>
<tr>
<td>2. Improve mindset and institutional culture to optimize problem solving capabilities and avoid the “failure of imagination”</td>
<td>Growing security subject matter expertise, aging workforce/tturnover</td>
<td>Avoid sensory data overload through use of tools like machine learning, data visualization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Streamlining data sharing, security clearance, access to necessary intelligence while balancing the need to protect critical infrastructure information</td>
<td>Expedite security clearances (which currently take 18+ months to process) and real-time intel sharing.</td>
<td>Expedite credible and accurate threat intel sharing through: (1) improvement of government declassification of information and (2) improvement of processes for sharing of information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Fully understanding adversary behavior: tactics, capabilities, tools, strategies, growing sophistication, identity of the adversaries; including insider threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Fully understanding stakeholder expectations</td>
<td>Engaging all customers in addressing security challenges, community buy-in.</td>
<td>Defining customer role in ensuring security; understanding true customer reliability expectations and cost sensitivity, including among different customer types (e.g. residential, business, CI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Overcoming inadequate cybersecurity workforce</td>
<td>Moving to 24/7 cybersecurity workforce</td>
<td>Attracting/retaining talent; Automation, AI, to support and enhance human capital; marketing breadth of opportunities; fully utilizing existing programs such as hackathons</td>
<td>Multidisciplinary approach required, educational pipeline insufficient bandwidth; university level education, short courses, summer schools</td>
<td>Communicating an inspirational vision (e.g. how to get people excited about internship at utility v. Apple or NASA)</td>
</tr>
</tbody>
</table>
# People #1 – 2

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ensuring a collaborative and consistent approach towards achieving a higher level of cyber and physical security</td>
<td>Building resiliency throughout ecosystem; growing employee skillset</td>
<td>Capability measurement: a. Baseline and advanced capabilities b. Drivers’ license type certification</td>
<td>Achieving a baseline level of cyber and physical security competency among all personnel</td>
<td>[input sought, if any]</td>
</tr>
<tr>
<td>2. Improve mindset and institutional culture to optimize problem solving capabilities and avoid the “failure of imagination”</td>
<td>Growing security subject matter expertise, aging workforce/turnover</td>
<td>Avoid sensory data overload through use of tools like machine learning, data visualization</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
</tbody>
</table>
### Challenges

3. Streamlining data sharing, security clearance, access to necessary intelligence while balancing the need to protect critical infrastructure information

### Opportunities

Expedite security clearances (which currently take 18+ months to process) and real-time intel sharing.

### Solutions

Expedite credible and accurate threat intel sharing through: (1) improvement of government declassification of information and (2) improvement of processes for sharing of information

### Education

" " " " " " " "

### Potential Action Items

" " " " " " " "
### People #5 - 6

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Fully understanding stakeholder expectations</td>
<td>Engaging all customers in addressing security challenges, community buy-in.</td>
<td>Defining customer role in ensuring security; understanding true customer reliability expectations and cost sensitivity, including among different customer types (e.g. residential, business, CI)</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
<tr>
<td>6. Overcoming inadequate cybersecurity workforce</td>
<td>Moving to 24/7 cybersecurity workforce</td>
<td>Attracting/retaining talent; Automation, AI, to support and enhance human capital; marketing breadth of opportunities; fully utilizing existing programs such as hackathons</td>
<td>Multidisciplinary approach required, educational pipeline insufficient bandwidth; university level education, short courses, summer schools</td>
<td>Communicating an inspirational vision (e.g. how to get people excited about internship at utility v. Apple or NASA)</td>
</tr>
</tbody>
</table>
BREAK
5 MINUTES
WORKING GROUP
PROCESS DISCUSSION
Figure 2: High-performing compliance organizations focus on four key elements

- **Role of compliance**
  - Aligned with regulations, business strategy and enterprise risk appetite
  - Clear principles and metrics that support this role

- **Enablers: People, processes, systems**
  - Right leadership skills, with strong performance management
  - Effective, efficient end-to-end processes, enabled by technology
  - Activities delivered out of most effective, lowest-cost environment

- **World-class compliance program**
  - Risk-based policies and standards
  - Well-defined and prioritized activities

- **Cross-functional operating model**
  - Clear roles, decisions and accountabilities
  - Supporting structure and organization design
  - Governance, monitoring and oversight
  - Ways of working and a culture of doing the right thing

Source: Bain & Company
<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Encouraging industry to gravitate toward adoption of a standardized set of approaches to increase operational efficiency</td>
<td>Trend towards adopting business practices even when not required because they make sense and are effective (e.g. NERC CIP, NIST, C2M2). Maturing risk management programs. DOE cybersecurity risk management process (RMP).</td>
<td>Formalize processes to certify people in best-practice use when interacting with OT and IT</td>
<td>[input sought, if any]</td>
<td>[input sought, if any]</td>
</tr>
<tr>
<td>2. Effectively measuring vendor capabilities, practices, and competencies when introducing their products into grid operations (including multiple tiers in the supply chain)</td>
<td>Securing supply chain and ensuring vendors incorporate and integrate security protection capabilities</td>
<td>Building resiliency throughout ecosystem; Supply chain security: Cloud, 3rd Party, and Consumer-grade Products</td>
<td>“ ” ”</td>
<td>“ ” ”</td>
</tr>
<tr>
<td>3. Address need for metrics to quantify effectiveness of interventions</td>
<td>Adoption of risk assessment and capability maturity models. Third-party assessment and continuous improvement.</td>
<td>Establish metrics for reliability, resiliency, and cybersecurity</td>
<td>“ ” ”</td>
<td>“ ” ”</td>
</tr>
<tr>
<td>4. Promoting an integrated return on investment strategy that includes physical and cyber security management (workforce, technology, process)</td>
<td>Ensuring security planning is incorporated in strategic planning and business processes; Potential valuation of resilience attributes in transmission planning</td>
<td>Incorporating change management into overall project plans</td>
<td>“ ” ”</td>
<td>“ ” ”</td>
</tr>
<tr>
<td>5. Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria</td>
<td>Promote increased cross-utility information sharing with regard to threat identification and incident response, complimentary to role of ISACs. Define need for information. Recognizing differing needs and goals.</td>
<td>Increased public private partnerships to facilitate information and best practices sharing. Enhancing operations across RTO seams (processes and tools); Responsive congestion management across RTO seams. Integrating emerging technologies to improve process.</td>
<td>“ ” ”</td>
<td>“ ” ”</td>
</tr>
<tr>
<td>6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities</td>
<td>Testing and exercising crisis and incident management capabilities across multiple jurisdictions</td>
<td>Exercise response capabilities through local, regional, and national coordinated exercises (CSIRT, GridEx, etc.)</td>
<td>“ ” ”</td>
<td>Continued development of ESCC Cyber Mutual Assistance program to coordinate between utilities in the event of an attack</td>
</tr>
<tr>
<td>Challenges</td>
<td>Opportunities</td>
<td>Solutions</td>
<td>Education</td>
<td>Potential Action Items</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>1. Encouraging industry to gravitate toward adoption of a standardized set of approaches to increase operational efficiency</td>
<td>Trend towards adopting business practices even when not required because they make sense and are effective (e.g. NERC CIP, NIST, C2M2). Maturing risk management programs. DOE cybersecurity risk management process (RMP).</td>
<td>Formalize processes to certify people in best-practice use when interacting with OT and IT</td>
<td>[input sought, if any]</td>
<td>[input sought, if any]</td>
</tr>
<tr>
<td>2. Effectively measuring vendor capabilities, practices, and competencies when introducing their products into grid operations (including multiple tiers in the supply chain)</td>
<td>Securing supply chain and ensuring vendors incorporate and integrate security protection capabilities</td>
<td>Building resiliency throughout ecosystem; Supply chain security: Cloud, 3rd Party, and Consumer-grade Products</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
<tr>
<td>Challenges</td>
<td>Opportunities</td>
<td>Solutions</td>
<td>Education</td>
<td>Potential Action Items</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>3. Address need for metrics to quantify effectiveness of interventions</td>
<td>Adoption of risk assessment and capability maturity models. Third-party assessment and continuous improvement.</td>
<td>Establish metrics for reliability, resiliency, and cybersecurity</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
<tr>
<td>4. Promoting an integrated return on investment strategy that includes physical and cyber security management (workforce, technology, process)</td>
<td>Ensuring security planning is incorporated in strategic planning and business processes; Potential valuation of resilience attributes in transmission planning</td>
<td>Incorporating change management into overall project plans</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
</tbody>
</table>
### PROCESS #5 – 6

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Opportunities</th>
<th>Solutions</th>
<th>Education</th>
<th>Potential Action Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria</td>
<td>Promote increased cross-utility information sharing with regard to threat identification and incident response, complimentary to role of ISACs. Define need for information. Recognizing differing needs and goals.</td>
<td>Increased public private partnerships to facilitate information and best practices sharing. Enhancing operations across RTO seams (processes and tools); Responsive congestion management across RTO seams. Integrating emerging technologies to improve process.</td>
<td>&quot; &quot; &quot;</td>
<td>&quot; &quot; &quot;</td>
</tr>
<tr>
<td>6. Prioritizing effective, regular, and consistent evaluation and testing of core capabilities</td>
<td>Testing and exercising crisis and incident management capabilities across multiple jurisdictions</td>
<td>Exercise response capabilities through local, regional, and national coordinated exercises (CSIRT, GridEx, etc.)</td>
<td>&quot; &quot; &quot;</td>
<td>Continued development of ESCC Cyber Mutual Assistance program to coordinate between utilities in the event of an attack</td>
</tr>
</tbody>
</table>
NEXT STEPS
NEXT STEPS

1. Whitepaper Sample and Template (WG Co-Leads and WG Members)

2. Submit content to Google Drive (WG Members and WG Co-Leads)

3. Review Priority Matrix and Remaining Topics Matrix (WG Members)

4. Distribute Regulatory & Compliance Matrices (WG Co-Leads)

5. Review and comment on notes from this session (WG Members)

6. Review and research topics for next session (WG Members)
FUTURE MEETINGS
FUTURE MEETINGS

Meeting #4 : May 22, 2018 (WebEx 9AM-12PM)
  • Regulatory and Compliance (and Any Carried Over Process Topics)

NextGrid Public Policy Meeting: June 14, 2018
  • Chicago 1PM-3:30PM
  • Public participation and presentations from all Working Group Leads
  • Optional 10AM-12Noon in-person WG3 meeting

Meeting #5 : June 25, 2018 (WebEx 12PM-3:30PM)
  • WG Report Discussion (WebEx)

Final Chapter Due : June 29, 2018
THANK YOU