Agenda

• Why the changes?
• What’s new?
• Example of a Risk Factor
• How does this effect CIP V5?
What Are Risk Factors?

Considerations used during an Inherent Risk Assessment (IRA) to identify a registered entity’s risk characteristics that are inherent to a registered entity’s configuration and may impact the reliability of the BPS.

- NERC IRA Guide
Use of Risk Factors in Risk Determination

Risk Element

Risk Factor 1
- Low
- Medium
- High

Risk Factor 2
- Low
- Medium
- High
Why are we changing the risk factors?

- CIP V3 to V5 transition
- Feedback from entities
- IRA process improvement
CIP V5

• Risk factors were updated based on V5
• Takes into account BCS (BES Cyber System) and the IRC (Impact Rating Criteria)
• Same risk principles still apply
Changes to Risk Factors
Current vs. New

Current risk factors
- Focused on numbers

New risk factors
- Not just numbers
- V5
- Considerations
- Quantitative and qualitative
Current Risk Factors

- Current risk factors focused on numbers
  - Personnel
  - Systems
  - Devices
  - Events
  - ESPs (Electronic Security Perimeters)
  - PSPs (Physical Security Perimeters)
New Risk Factors

• New risk factors
  – Moving away from just using numbers
  – Systems, V5 impact, locations of BCS (BES Cyber System) Facilities
  – Considerations that help identify entities who might be on the edge of low, medium, or high risks
  – Moving away from quantitative to a combination of quantitative and qualitative factors
Risk Factor Process

• Compliance Risk Analysis team worked with many groups during the risk factor process
  – CIP and O&P audit teams
  – RAPA (Reliability Assessment Performance Analysis) working group
  – Industry

• Research in the areas of cyber security and O&P risks
Current & New CIP Risk Factors

**Current**
- Critical Asset Identification
- System Complexity
- System Access
- Cyber Security Events
- Physical Access

**New**
- BCS Identification
- System Management
- Cyber Security Incidents
- Physical Access
New Risk Factor Example

Physical Access
New Risk Factor Example

Physical Access

- PSP changes
- PSPs by site
- PSP design
Physical Access Example

Physical Access

PSP changes
- No changes
- Minor changes
- Major changes

PSPs by site
- < 3 per site
- 3 – 7 per site
- > 7 per site

PSP design
- PSPs are within 5 mile radius
- PSPs are within 6-20 mile radius
- PSPs greater than 20 mile radius
Physical Access Example

- PSP changes (since last audit)

- Low: No PSP changes
- Medium: Minor PSP changes
- High: Major changes
Physical Access Example

- PSPs by site – number of PSPs by site

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>&lt; 3 per site</td>
</tr>
<tr>
<td>Medium</td>
<td>3 – 7 per site</td>
</tr>
<tr>
<td>High</td>
<td>&gt; 7 per site</td>
</tr>
</tbody>
</table>
Physical Access Example

- PSP design - geographic dispersion

**Low**
PSPs are within 5 mile radius

**Medium**
PSPs are within 6-20 mile radius

**High**
PSPs greater than 20 mile radius
Physical Access Considerations

• Type of PSP change
  – total redesign vs. removing an access point

• Size and attack surface
  – small PSP design vs. large PSP design and number of sites with PSPs

• Dispersion of PSP sites, size of guard force, how you work with local law enforcement
Physical Access Rating Example

- No PSP changes since last audit
- 9 PSPs at one site
- PSPs are greater than 20 mile radius
- Work with local law enforcement for quick response time for locations further away from local guard force
Physical Access Rating Example

• We have the thresholds
• Entity provided information
• Use considerations and professional judgment
Physical Access Rating Example

Low

PSP changes

High

PSPs by site

High

PSP design
Overall Risk Score

• Consider
  – Guard force
  – Local law enforcement
  – Response times
  – PSP design, small PSPs with minimal access, layers of physical constraints

• Physical Access = Medium
Summary

• Impact of CIP V5
• New risk factors
• Examples
• Considerations
Resources

• ERO 2016 CMEP IP
• WECC 2016 Draft CMEP IP
• WECC IRA Process
Speaker Contact Info

Ben Christensen
Senior Compliance Risk Analyst, Cyber Security
801-819-7666
bchristensen@wecc.biz