Hosted By:

ENERGYSEC
SERVING THE INDUSTRY´S SECURITY COMMUNITY SINCE 2004

Sponsored By:

Honeywell

Get Ready For Version 4

March 27 2013
Webinar

Welcome!

- Why are we doing this webinar?
  - The transition from CIP v3 to v4 is widely misunderstood
  - Many utilities will be identifying their 1st Critical Asset
  - Identifying essential cyber assets needs more explanation

- Today's agenda:
  - The CIP v4 Timetable / Tom Alrich
  - Getting Started with CCA Identification / Donovan Tindill
  - What's Most Important in CIP v4 / Steve Parker

Your Presenters

Tom Alrich is part of the Honeywell Process Solutions industrial cyber security team, focusing on the energy sector and especially electric power. He has been involved with industrial cyber security and especially NERC CIP compliance since 2008. Tom has spent most of his career in the IT industry, primarily in services for networking and cyber security. Tom has a BA in Economics from the University of Chicago. He lives in Evanston, Illinois.

Donovan Tindill is a Senior Security & Compliance Consultant at Honeywell. For over 13 years, Donovan has specialized in cyber security for industrial automation & control systems (IACS) to a wide variety of industries. Donovan has been involved with NERC CIP compliance since 2005, from the Urgent Action standards through to the latest CIP version 5 drafts. Additionally, he supports ISA99/IEC62443 as a contributor, committee leader and co-chair of Working Group 6 on IACS patch management.

Steven Parker is President of Energy Sector Security Consortium (EnergySec). He was part of the grassroots effort that led to the formation of EnergySec, and has served on its board of directors since 2008. Steven holds the CISA and CISSP certificates. Steve was formerly a Senior CIP Compliance Auditor at WECC and has implemented the CIP standards as an employee of a large utility in the Western US.

Your host: **Stacy Bresler**. Currently, the co-principal investigator for the National Electric Sector Cybersecurity Organization and the Vice-President of Outreach and Operations at EnergySec.

Today's Agenda

□ The CIP v4 Timetable / Tom Alrich

□ Getting Started with CCA Identification / Donovan Tindill

□ What's Most Important in CIP v4 / Steve Parker

□ Final Q&A

Timetable for CIP Version 4

- The process of developing CIP V4 and V5 has been ongoing since 2010.
- I have been continually thinking I was sure what the timetable would be.
- I have continually been wrong – at least 6 or 7 times I've had to revise what I thought would happen.

What's Today's Timeline?

This is what we know:

- CIP Version 4 is approved by both NERC and FERC.
- Compliance date is April 1, 2014.
- This is for compliance with all standards: CIP-002-4 through CIP-009-4.*
- * For assets in service in June of 2012.

What about Version 5?

- The Version 5 implementation plan says it will supersede Version 4 when approved by FERC.
- Ain’t gonna happen – see blog post.
- Nobody wanted to have two new versions, but that is what we will have.
- V5 will still likely come into effect in 2016 or 2017. You should start thinking about that as well – capital projects, etc.

NERC's Latest 'Plan'

- NERC discussed a new Version 4 / Version 5 "Transition Plan" three weeks ago – it will probably be out in final form soon.
- I saw the original presentation at the March CIPC meeting.
- I and many others think it is seriously flawed.
- It may be improved, but it won't change the fact: Version 4 will come into effect 4/1/2014.

My suggestion to NERC and FERC

- I have suggested that NERC petition FERC to push back the Version 4 implementation date by a year. This is my personal recommendation.
- This is because of confusion due to mixed messages from NERC (and other reasons – see my blog post from January).
- I hope this happens, but I have no idea whether it will. Don't bank on this either.

What Does ‘Compliance’ Mean?

- Some have asked whether 4/1/2014 is the Compliant or Auditably Compliant date. These are CIP V1 terms – 4/1/2014 is the Compliant and Auditably Compliant date for Version 4.
- This means you have to have everything for compliance in place on that date.
- Includes all policies, procedures and technologies in CIP-003 through CIP-009.

‘Bookending’

- For some requirements (requiring annual compliance), entities need to perform certain actions before 4/1/2014.
- Examples: Security policy (CIP-003 R1.3), Information Protection program (CIP-003 R4.3), training (CIP-004 R2), PRA’s (CIP-004 R3), Cyber vulnerability assessment (CIP-005 R4), Physical access controls testing (CIP-006 R8.1 and R8.2, etc).

What about IPNICCANRE?

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

- There are some who believe that assets identified by the V4 criteria are "newly identified" under V4 – thus they have 6-24 more months to comply after 4/1/2014.
- They are wrong; NERC and the RE's are in agreement on this.
- It's too complicated to explain here: see my Jan. post at http://tomalrichblog.blogspot.com/

Today's Agenda

✓ The CIP v4 Timetable / Tom Alrich

□ Getting Started with CCA Identification / Donovan Tindill

□ What's Most Important in CIP v4 / Steve Parker

□ Final Q&A

Getting Started with CCA Identification

- The owner-defined risk-based assessment methodology (RBAM) from CIP-002-3 is replaced with the industry-defined Attachment 1 Critical Asset Criteria (aka. the “bright-line” criteria).
  - To complete this, will require coordination with your Balancing Authority, Transmission Planners, Reliability Coordinator, ISO, Engineering teams, and others.

- Once the list of Critical Assets are identified, we can proceed with the identification of Critical Cyber Assets.

- The process described in the upcoming slides assumes no prior CIP compliance at the facility and you probably weren’t around for CIP-002-1.
  - Process is suitable for small or large organizations. Proven on large electric utilities (Example 1: over 11 sites; over 1500 Cyber Assets).

Process Overview

Assumes 1 or more Critical Assets exist.

A. Identify Essential Functions of the Critical Asset
B. Develop Preliminary Cyber Asset List and Prepare for Inventory
C. Perform Onsite Cyber Asset Inventory
D. Develop Detailed Cyber Asset List
E. Identify Cyber Assets that are Essential to the Critical Asset
   - □ Generation-Only: Determine the megawatts (MW) affected and minutes to impact for each shared Cyber Asset.

F. Determine the Qualifying Connectivity of each Cyber Asset (Sketch Preliminary ESP)
G. Implement Engineering Changes to Modify Impact/Connectivity/Scope
H. Verify and Approve the List of Critical Cyber Assets

This **is** your project plan!

A. Identify Essential Functions

Generation	Transmission	Control Centers
•Supervision and Control (Governor, Frequency, Voltage, AGC, etc.) •Dynamic Response •Startup, Shutdown •Exciter **Secondary Systems**: •Water Treatment •Fuel Source (Gas Pipeline, Coal Handling, Storage, etc.) •Emissions Control, Fly Ash	•Balancing Load & Generation •Dynamic Response •BPS Restoration •Protection (Voltage, Frequency, Phase, etc.) •Control (Frequency, Voltage, etc.) •Special Protection Systems (SPS) •Remedial Action Scheme (RAS) •Load Shedding	•Remote Supervisory and Control Remote control of >1500MW, 1000MV, Blackstart, 500kV, SPS, RAS, and others… •Real-time Operational Decision Making, Situational Awareness •Real-time Inter-utility Data Exchange, Inter-Entity Coordination •Managing Constraints •Dynamic Response

Lessons Learned:

– Involvement of site staff (e.g., Engineering, Maintenance) is essential to the accurate identification of Cyber Assets associated with the functions above.

References:
-NERC Guideline for Identifying Critical Assets: http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdfm Table C-1 Transmission Substations, Table C-2 Generation, Table C-3 Control Centers.
-Definition of Adequate Level of Reliability (ALR): http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf
-BES Reliability Operating Services: http://www.nerc.com/docs/standards/sar/CIP-002-5_clean_4_(2012-1024-1100).pdf, pages 17-22.

B. Preliminary List and Prepare for Inventory

1) **Preliminary Cyber Asset List** - Based on the list of essential functions, have Site Personnel draft a list. Use this for effort estimates, scheduling, and planning.

2) **Prepare Site Inventory Plan** - *To determine the approach, methodology, level of detail, templates, and resources required to inventory and characterize each facility.*
   - Determine the facility sizes and estimate the Cyber Asset counts. Identify those having a prior CIP compliance program, and the state of their Cyber Asset List, PSP and ESP documentation.
   - Project planning, resource estimating, schedule planning. Determine if facilities will be visited in series, or parallel, and how many.
   - Prepare checklists, data entry templates, examples, and other job aids to ensure information is collected consistently and accurately.
     - Interview questionnaires, Cyber Asset list, data collection checklists (per facility, per room, per network, per Cyber Asset), ESP/PSP drawing templates, etc.
     - Automated data collection scripts, manual collection entry forms

Lessons Learned: Host a boot camp for project participants.

C. Onsite Cyber Asset Inventory

- Visit each facility to perform detailed site inventory.
  - Requires at least 2 people (Site Expert, and Expert on both Technology and CIP).
  - Physically inspect, manual and electronic collection, communication connectivity, impact to essential functions. Over-collect information as it may be required for CIP compliance later.
  - Make, model, serial number, IP address, photos, firmware/software versions, installed software, users, security capabilities, etc.
  - Both logical (IP, MAC, network interfaces, MAC address tables) and physical cable tracing
  - Interviewing and other information related to essential functions and relationship to Cyber Assets. Ask about minutes to impact.

- Lessons Learned:
  - Cyber Assets not previously inventoried need budgeted >1 hour each!
    - Actual Site Inventory Labor: 11 sites, 1500 Cyber Assets = 2,200 hours
  - Site inventory can uncover >30% more assets than originally thought!
  - Existing network drawings >2 years old cannot be trusted, easier to start over with both logical and physical cable tracing.
  - Spend lots of time asking about impact, and possible engineering changes.

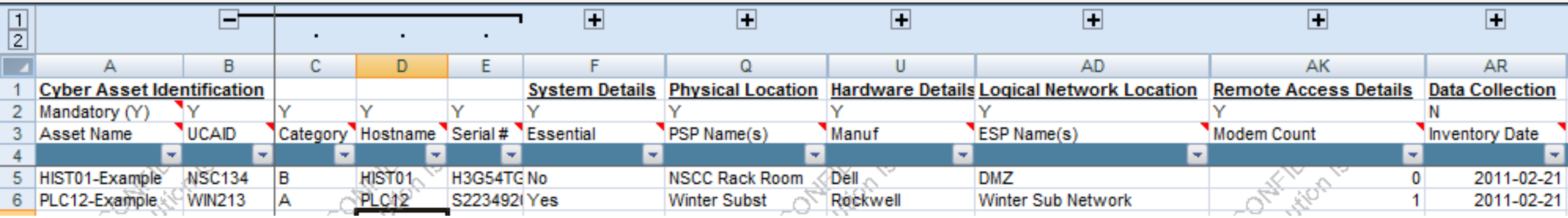
Typical Cyber Assets Found

Generation	Transmission	Control Centers
•Servers, Operator Workstations, Engineering Workstations, Laptops, Historian, Web Servers •Routers, Switches, Hubs, Media Convertors, Telecom Equipment in Electrical Switching Rooms •Fly Ash and Coal Handling Operator Stations •Environment Monitoring, Vibration Monitoring, Revenue Meters, Water Lab •Vendor Remote Access (e.g., dial-up modems, WAN routers) •AGC (Auto-Generation Control) •PLCs, Controllers	•Telecom WAN equipment (e.g., serial, T1) •Network Switches •Dial-Up Modems •Protection Relays (aka. RTUs) •Local HMI •Touch Displays	•Servers •ICCP Relay Servers •Operator Workstations, Engineering Workstations •Firewalls, Routers, Switches •Front-End Processors, Serial-to-Ethernet Convertors, Terminal Servers •Heads-Up Wall-Panel Display PCs •Inter-Utility Network Access Routers

Lessons Learned:

– 50% of equipment is non-IT traditional infrastructure. Not easily recognized nor information easily collected.

D. Develop Detailed Cyber Asset List



	A	B	C	D	E	F	Q	U	AD	AK	AR
1	**Cyber Asset Identification**					**System Details**	**Physical Location**	**Hardware Details**	**Logical Network Location**	**Remote Access Details**	**Data Collection**
2	Mandatory (Y)	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
3	Asset Name	UCAID	Category	Hostname	Serial #	Essential	PSP Name(s)	Manuf	ESP Name(s)	Modem Count	Inventory Date
4											
5	HIST01-Example	NSC134	B	HIST01	H3G54TG	No	NSCC Rack Room	Dell	DMZ	0	2011-02-21
6	PLC12-Example	WIN213	A	PLC12	S223492(	Yes	Winter Subst	Rockwell	Winter Sub Network	1	2011-02-21

- Includes the basics required for CIP compliance and CCA determination
  - Purpose, Hostname, Serial#, IP, Location, Modems,
- Should also contain information to support CIP-003 thru CIP-009 (if expected)
  - Owner, Administrators, TFEs Expected, Operating System, Versions, Can it be rebooted, antivirus installed, software installed, users, etc.

Lesson Learned: Cheaper to collect too much on first visit versus collecting a second time!

E. Essential Cyber Asset Identification

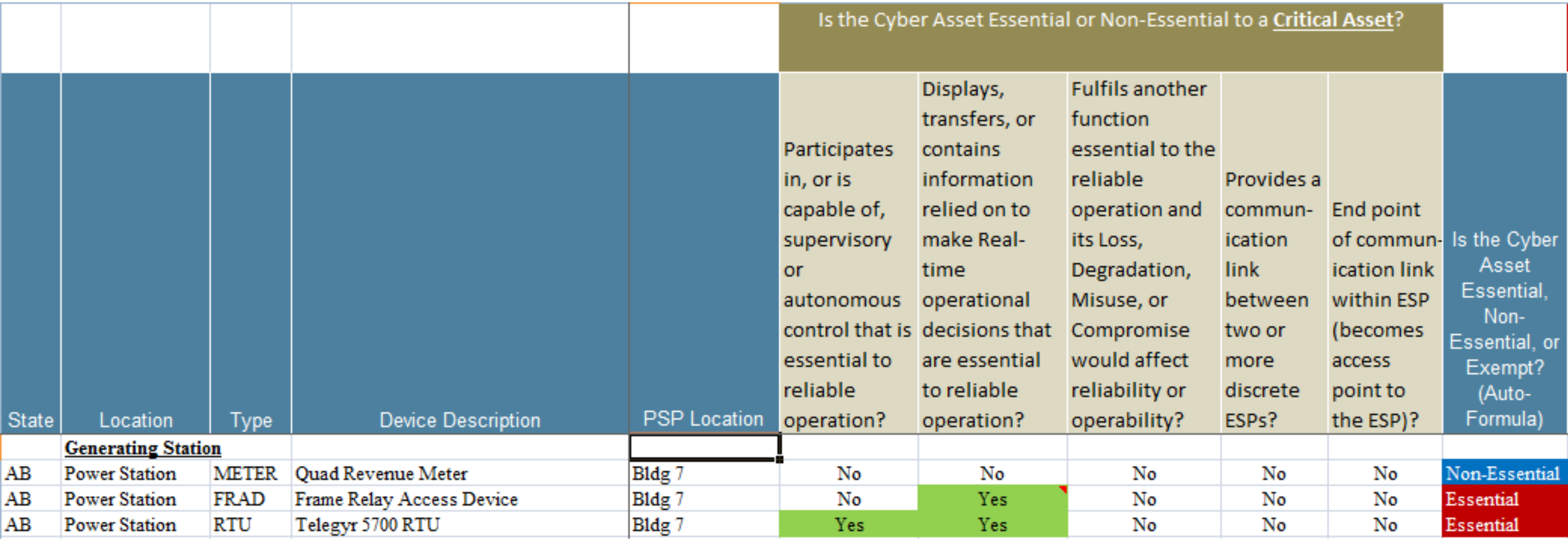
- Factors determining whether a Cyber Asset is "essential":
  - □ The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.
  - □ The Cyber Asset displays, transfers, or contains information relied on to make real-time operational decisions that are essential to the reliable operation of a Critical Asset.
  - □ The Cyber Asset fulfils another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BES.
  - □ If the Cyber Asset was compromised, tampered with, produced erroneous data, or operated maliciously, this would affect the reliable operation of the Critical Asset immediately or over time.
  - □ If there is a Loss, Degradation, or Compromise of the essential Cyber Asset, within how much time is the plant adversely impacted? If within 15 minutes, then the Cyber Asset is further considered.
  - □ Generation Only: If the essentially Cyber Asset does potentially have an adverse impact within 15 minutes, are there any technical or procedural changes that could be made to reduce the megawatts affected, or to increase the time for adverse impact to be realized? (This is only to assess options to reduce the potential number of critical cyber assets.)

E. Essential Cyber Asset Identification

- Other factors that determine if the Cyber Asset is “non-essential”:
  - ❑ If these Non-Essential Cyber Asset(s) fail, there is sufficient indication and warning to allow remedial actions to be taken within 15 minutes.
  - ❑ Information supplied by these Non-Essential Cyber Asset(s) is **not** used in operational decisions, and is verified procedurally to prevent impacts upon the Critical Asset. For example, monitoring information may indicate the health of equipment but it would be procedurally verified to confirm the condition before making any decisions that may affect operations.
  - ❑ These Non-Essential Cyber Asset do not have a direct connection to the control system such that they would not impact an essential function. For example, the non-essential system does not prevent the startup, operation, or safe shutdown of the Critical Asset.

- Lessons Learned:
  - – Answer **every** question for **every** Cyber Asset. Have Engineering and Maintenance teams provide the technical responses.
  - – Having the technical response for every Cyber Asset expedites the **annual review** process, and virtually eliminates any skepticism during the audit process.

Example Worksheet: Identification of Essential Cyber Assets



					Is the Cyber Asset Essential or Non-Essential to a Critical Asset?					
State	Location	Type	Device Description	PSP Location	Participates in, or is capable of, supervisory or autonomous control that is essential to reliable operation?	Displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to reliable operation?	Fulfils another function essential to the reliable operation and its Loss, Degradation, Misuse, or Compromise would affect reliability or operability?	Provides a communication link between two or more discrete ESPs?	End point of communication link within ESP (becomes access point to the ESP)?	Is the Cyber Asset Essential, Non-Essential, or Exempt? (Auto-Formula)
	Generating Station									
AB	Power Station	METER	Quad Revenue Meter	Bldg 7	No	No	No	No	No	Non-Essential
AB	Power Station	FRAD	Frame Relay Access Device	Bldg 7	No	Yes	No	No	No	Essential
AB	Power Station	RTU	Telegyr 5700 RTU	Bldg 7	Yes	Yes	No	No	No	Essential

- Screenshot above has been edited for screen size, should include 8 criteria from prior 2 slides

Lessons Learned:

- Have a supporting document containing the detailed engineering response to each Yes/No answer. Update annually.
- Document the minutes to impact for each.

F. Qualifying Connectivity

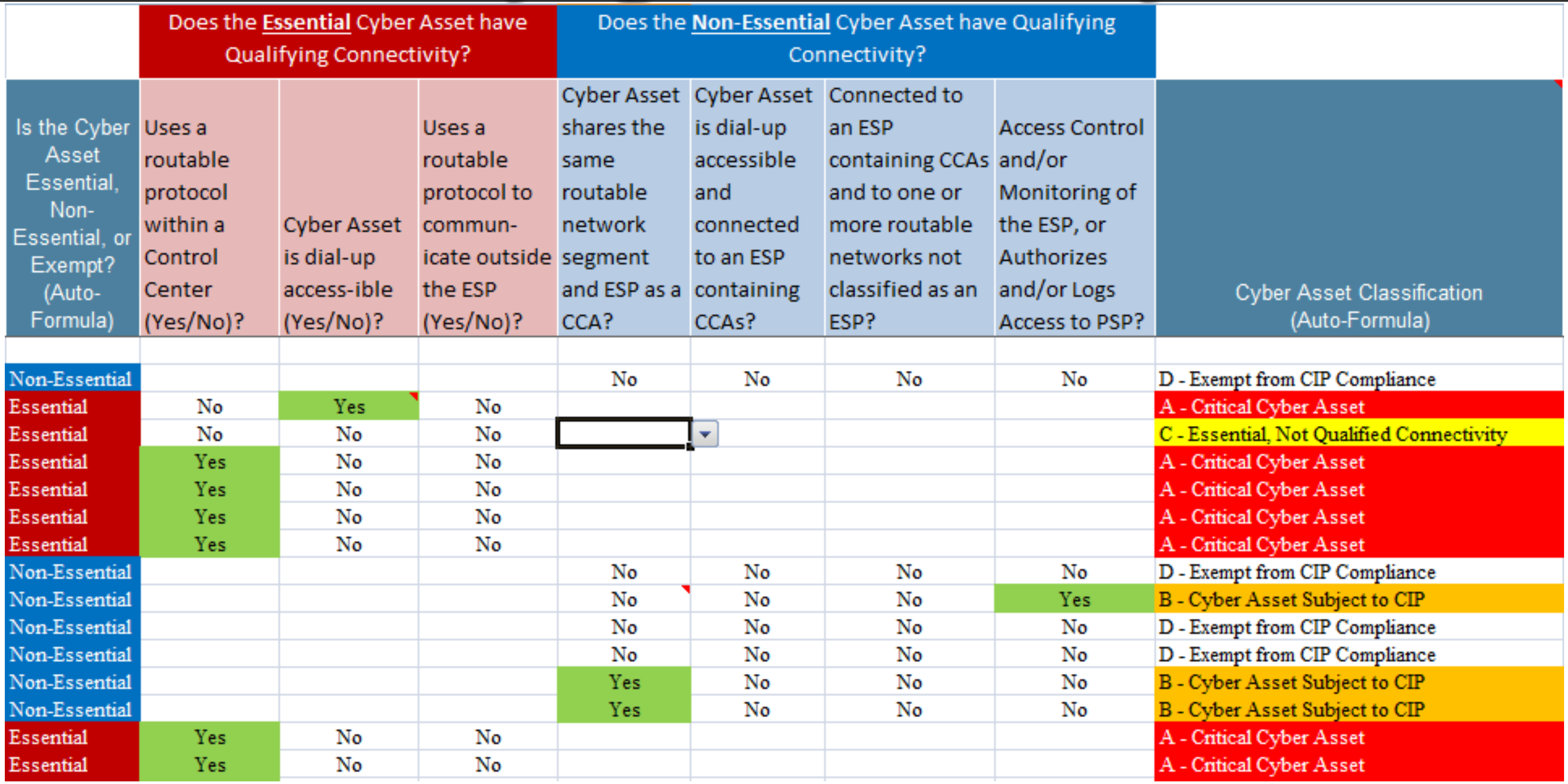
- Does the essential Cyber Asset have qualifying connectivity?
  - The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
  - The Cyber Asset uses a routable protocol within a control center; or,
  - The Cyber Asset is dial-up accessible.

- Is there an access point, resulting in communication outside the ESP?
  - CIP-005 R1.1: Includes any externally connected end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter.
  - Cyber Asset is dial-up accessible and connected to an Electronic Security Perimeter containing Critical Cyber Assets.
  - Cyber Asset is connected to an Electronic Security Perimeter containing Critical Cyber Assets and to one or more routable networks not classified as an Electronic Security Perimeter.

- Lessons Learned:
  - Isolated networks don't have access points; doesn't apply to Control Centers.
  - Generation: Historians are the single biggest reason access points to the ESP exist!
  - Transmission: Serial connectivity to relays/RTUs is your best technology choice at this time.
  - How to un-engineer an access point:
    - Objective 1: Ensure there is no impact (e.g., block writes, block configure)
    - Objective 2: Avoid routable and dial-up technologies.
    - Objective 3: Implement technical or procedural measures to increase impact >15 minutes.

References:
-NERC Guideline for Identifying Critical Cyber Assets:
http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCI%20and%20SC%20for%20Posting%20with%20CIP-002-1.%20CIP-002-2,%20CIP-002-3.pdf.

Example Worksheet: Qualifying Connectivity



	Does the **Essential** Cyber Asset have Qualifying Connectivity?			Does the **Non-Essential** Cyber Asset have Qualifying Connectivity?				
Is the Cyber Asset Essential, Non-Essential, or Exempt? (Auto-Formula)	Uses a routable protocol within a Control Center (Yes/No)?	Cyber Asset is dial-up access-ible (Yes/No)?	Uses a routable protocol to commun-icate outside the ESP (Yes/No)?	Cyber Asset shares the same routable network segment and ESP as a CCA?	Cyber Asset is dial-up accessible and connected to an ESP containing CCAs?	Connected to an ESP containing CCAs and to one or more routable networks not classified as an ESP?	Access Control and/or Monitoring of the ESP, or Authorizes and/or Logs Access to PSP?	Cyber Asset Classification (Auto-Formula)
Non-Essential				No	No	No	No	D - Exempt from CIP Compliance
Essential	No	Yes	No					A - Critical Cyber Asset
Essential	No	No	No					C - Essential, Not Qualified Connectivity
Essential	Yes	No	No					A - Critical Cyber Asset
Essential	Yes	No	No					A - Critical Cyber Asset
Essential	Yes	No	No					A - Critical Cyber Asset
Essential	Yes	No	No					A - Critical Cyber Asset
Non-Essential				No	No	No	No	D - Exempt from CIP Compliance
Non-Essential				No	No	No	Yes	B - Cyber Asset Subject to CIP
Non-Essential				No	No	No	No	D - Exempt from CIP Compliance
Non-Essential				No	No	No	No	D - Exempt from CIP Compliance
Non-Essential				Yes	No	No	No	B - Cyber Asset Subject to CIP
Non-Essential				Yes	No	No	No	B - Cyber Asset Subject to CIP
Essential	Yes	No	No					A - Critical Cyber Asset
Essential	Yes	No	No					A - Critical Cyber Asset

Lessons Learned: Have a supporting document containing the detailed engineering response to each Yes/No answer. Update annually.

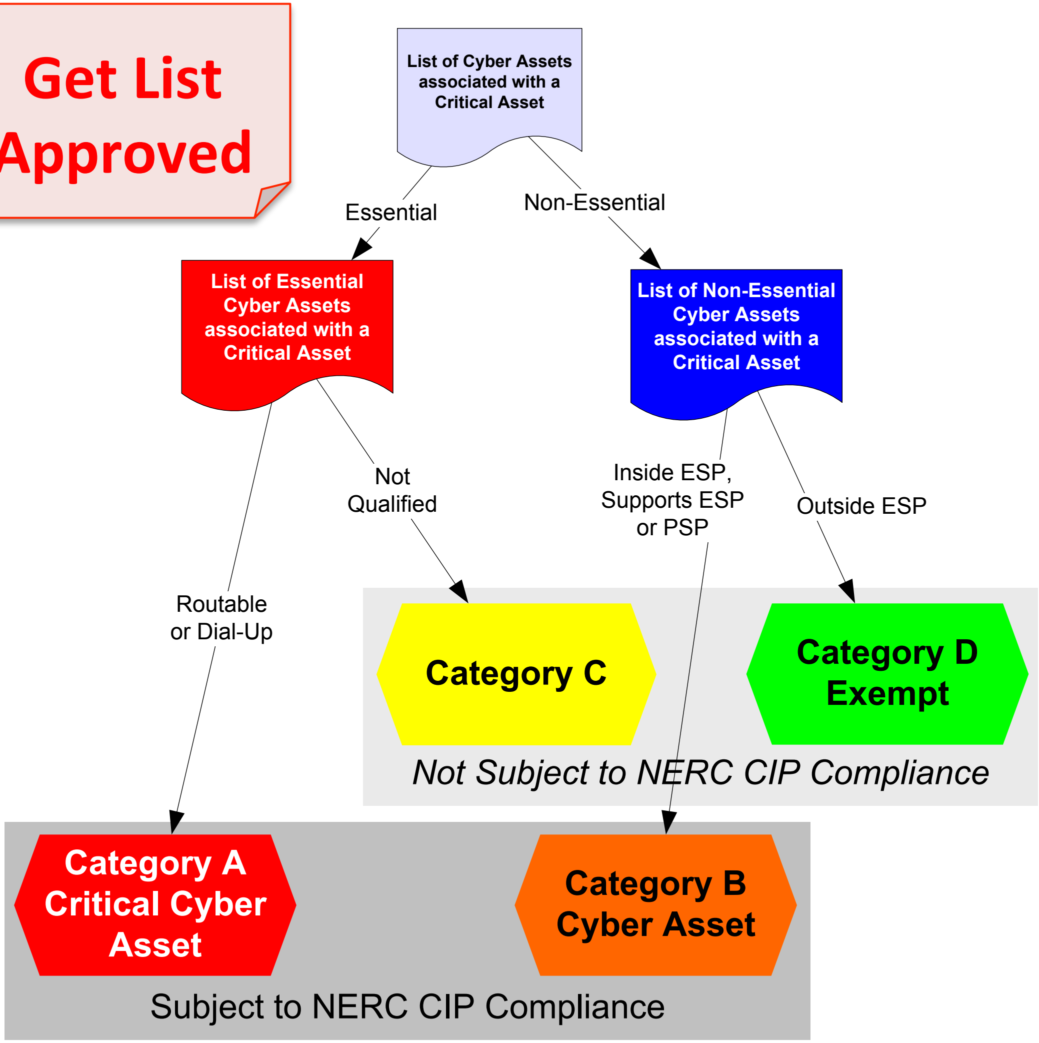
CCA Identification Summary

- **CCA** - Cyber Asset that is essential to the operability or reliability of the Critical Asset and has qualifying connectivity requiring compliance with CIP-002 through CIP-009.

Get List Approved

- **NCCA (B)** - Cyber Asset is not essential, but is subject to varying levels of CIP-002 through CIP-009 compliance due to a function supporting the ESP or PSP, or its connectivity in relationship to Critical Cyber Assets. E.g., NCCA, EACMS, PACMS, etc.

- **Category C** - Cyber Asset supports an essential function of the Critical Asset, but does not have qualifying connectivity and is exempt from CIP-003 through CIP-009 compliance.
- **Category D** - Cyber Asset is explicitly exempted, does not support an essential function, does not have qualifying connectivity, and is exempt from CIP-002 through CIP-009 compliance



List of Cyber Assets associated with a Critical Asset

Essential

Non-Essential

List of Essential Cyber Assets associated with a Critical Asset

List of Non-Essential Cyber Assets associated with a Critical Asset

Not Qualified

Inside ESP, Supports ESP or PSP

Outside ESP

Routable or Dial-Up

Category C

Category D Exempt

Not Subject to NERC CIP Compliance

Category A Critical Cyber Asset

Category B Cyber Asset

Subject to NERC CIP Compliance

Methodology & Schedule

Phase	Minimum Schedule	Applicability
1: Planning and Preparation	Now	Everyone
2: Field Inventory and CCA Identification	1-3 months	Everyone
3: Scoping, Design & Engineering, Detailed Project Planning	1-4 months	If CCAs
4+: Achieve Compliance *or Engineering Changes* ❑Procurement, Build, Integration, Test, Document, etc. ❑ESP, PSP, CIP7 Infra, CIP9 Infra ❑Harden existing Cyber Assets ❑Process, Procedures, Training, Institutionalization	6-24 months	If CCAs
5: Verify (Find and Fix)	1-3 months	If CCAs
Compliant	**April 1, 2014**	

Today's Agenda

- ✓ The CIP v4 Timetable / Tom Alrich
- ✓ Getting Started with CCA Identification / Donovan Tindill
- ☐ What's Most Important in CIP v4 / Steve Parker
- ☐ Final Q&A

What’s Most Important in V4

- Key Points
  - – CIP-003 thru CIP-009 are unchanged
  - – Bright lines may result in new Critical Assets
  - – Many requirements take time to implement
  - – Begin planning to establish timelines

Where to Start

- Identify assets that will be in-scope
- Establish CIP governance and policies
- Identify staff for implementation tasks
- Establish a project plan and schedule

Focus Areas for New Critical Assets

- Perimeters (Electronic and Physical)
- Access Control
- Logging
- Technical Feasibility Exceptions

Perimeter

- Electronic
  - Rulesets. Identifying required ports/services
  - Technical designs
  - Remote Access
  - Logging and Monitoring
- Physical
  - Security Plan
  - Construction timelines

Access Control

- Process
  - Approvers and approval process
  - Documentation and review of rights
- Technical controls
- Password rules

Logging

- Perimeters
- System Logs
- Technology design and/or acquisition
- Staffing

Technical Feasibility Exceptions

- Identify eligible assets
- Prepare documentation
- Develop mitigations (compensating controls)
- Submit Requests

Today's Agenda

✓ The CIP v4 Timetable / Tom Alrich

✓ Getting Started with CCA Identification / Donovan Tindill

✓ What's Most Important in CIP v4 / Steve Parker

□ Final Q&A

Contact Us

- Email: Stacy Bresler (stacy@energysec.org)
- Email: Tom Alrich (tom.alrich@honeywell.com)
- Email: Donovan Tindill (donovan.tindill@honeywell.com)
- Email: Steve Parker (steve@energysec.org)

- Website: www.energysec.org
- Website: www.becybersecure.com

- Blog: InSecurity.honeywellprocess.com
- Blog: TomAlrichBlog.blogspot.com

- Twitter: EnergySec; InSecCulture; DTindill;
- LinkedIn: All of us

Thank you!

ENERGYSEC
SERVING THE INDUSTRY´S SECURITY COMMUNITY SINCE 2004

Upcoming NERC CIP Training Opportunities:

June 11 | Chicago, Il
NERC CIP-005/CIP-007 Deep Dive Training
Register - http://grids.ec/CIPDeepDive

June 19-20 | Knoxville, TN
NERC CIP Compliance Bootcamp
Register - http://grids.ec/CIPBootcamp

October 9 | Dallas, Tx
NERC CIP-005/CIP-007 Deep Dive Training
Register - http://grids.ec/DallasCIPTraining

December 4 | Sacramento, CA NERC CIP-005/CIP-007
Deep Dive Training
Register - http://grids.ec/SacCIPTraining

Honeywell

For more information about Honeywell's Vendor-Independent Cyber Security and NERC CIP services:

www.becybersecure.com