Critical Infrastructure Protection:
Do you know where your Critical Cyber Assets are?

June 6, 2006
Legacy SCADA Design

- Communications Media
  - Wire Line (leased or private)
  - Fiber Optic
  - Wireless (Pt. - Pt. Microwave, ISM, 802.11)
  - Other
- Protocols: Serial Byte-Asynchronous
  - Legacy Proprietary
  - Open (Modbus, DNP, UCA, TG8979)
- Data Rate: 9600 BPS Typ.
Interoperable

- Thin Client HMIs
  - Web front ends
  - Remote Management
  - Minimal processing requirements
- COTS Enterprise Servers
  - Microsoft, Linux based OS
  - Patches and updates require vendor certification
- IP based Comms
  - Interconnectivity with corporate networks and 3rd parties
- Smart Devices
  - Embedded Microsoft OSs
  - Remotely administered
- More Vulnerable
What is a Critical Cyber Asset?

• **Hint** - Not just control centers anymore
CCA Level-Setting

Ratios of CCAs to CA: Average 3:1

- Criticality is measured by a cyber asset’s function (i.e. control) in relation to critical assets.

- Routable protocols are a required filter for NERC CIP but should be used as the final determinant.

- SEL relays that are not IP-enabled behind an “IP” relay gateway?? Are these CCAs?
Determining Cyber Asset Decision Flow

1. Is the facility on the Critical Asset (CA) list?
   - NO
     - Stop Catalogue asset as non-critical and reapply during annual re-assessment for changes.
   - YES

2. Is there an inventory of electronic assets available?
   - NO
     - Create list and move to 3
   - YES

3. Are there electronic assets with a routable protocol?
   - NO
     - Are there assets which are accessible via dial-up modems?
     - NO
       - Stop Catalogue asset as non-critical and reapply during annual re-assessment for changes.
     - YES
       - Go to non-Control Center flow
   - YES
     - Go to Control Center flow

4. Are there assets which are accessible via dial-up modems?
   - NO
     - Go to Control Center flow
Control Center Critical Cyber Asset Decision Flow

1. From Determine Asset flow
   - Does the system have an application that performs the following types of functions? Includes but is not limited to:
     - State Estimator
     - Area Control Error
     - Automatic Generator Control
     - Breaker Control
     - Or any other function that is otherwise considered to be part of an Energy Management System
     - Voltage Regulator
     - Turbine control
     - Burner Management Boiler Control
   - Yes → Include on the Critical Cyber Asset (CCA) List (red)
   - No

2. Yes → Include on CCA List (red)
   - No

3. Does the system have data required to perform the functions listed in #2? Includes but not limited to:
   - Databases
   - Spreadsheets
   - Other Flat Files
   - Yes → Include on CCA List (red)
   - No

4. Does the systems contain source code for applications that support functions in #2 and #3?
   - Yes
     - No → Include on CCA List (red)
     - Yes
   - No → Does the system provide an application interface or is otherwise considered to be the primary workstation of an operator/dispatcher?
     - Yes
       - Yes → Include on CCA List as yellow (protected like a CCA but not a CCA)
       - No → Catalogue asset and re-apply assessment annually.
     - No → Include on CCA List (red)

5. No → Does the system provide an application interface or is otherwise considered to be the primary workstation of an operator/dispatcher?
   - Yes
     - Yes → Include on CCA List as yellow (protected like a CCA but not a CCA)
     - No → Catalogue asset and re-apply assessment annually.
   - No → Include on CCA List (red)

6. Does the system provide a toolset, graphs, or otherwise provide material support to operator functions? “Material” Defined as those tools that if unavailable would have an immediate impact on system reliability. Includes but is not limited to:
   - Graphs, charts, spreadsheets etc. that support decision making functions where otherwise unavailable in systems provided in Step 1
   - Material may be available in the EMS but no one knows how to use it.
   - Yes → Include on CCA List (red)
   - No

7. Is the system a “networking component” that supports the network of CCAs or otherwise defines the Electronic Security Perimeter for CCAs? Includes but is not limited to:
   - Firewalls
   - Routers
   - Switches
   - Yes → Include on CCA List (red)
   - No

8. Is the system, if not otherwise a CCA, on the same logical network within the same electronic security perimeter as CCAs?
   - Yes → Include on CCA List (red)
   - No

Include on CCA List as yellow (protected like a CCA but not a CCA)
The new face of Critical Cyber Assets

- RTUs, Relays & Communication Processors

- Controllers, PLCs, and HMIs
  - Emerson’s Migration path from WDPF includes upgrading controllers with embedded VxWorks.
  - Controllers are IP enabled
Dual Homed Systems, IP-enabled Controllers, and Vendors

...OH MY!

(Generation Critical Cyber Assets)
And now for something completely different.....

(Substation Critical Cyber Assets)
Thank You

Ben Church, CISSP
Burns & McDonnell
bchurch@burnsmcd.com