Confidential

Audit Overview

December 4, 2012

Randi Nyholm
Transmission Compliance Specialist, Senior
(218) 723-7466
rnyholm@mnpower.com

minnesota power
AN ALLETE COMPANY

Agenda

- Preparation
- Audit Process
- On-Site Audit
- What Comes Next
- Best Practices

Confidential

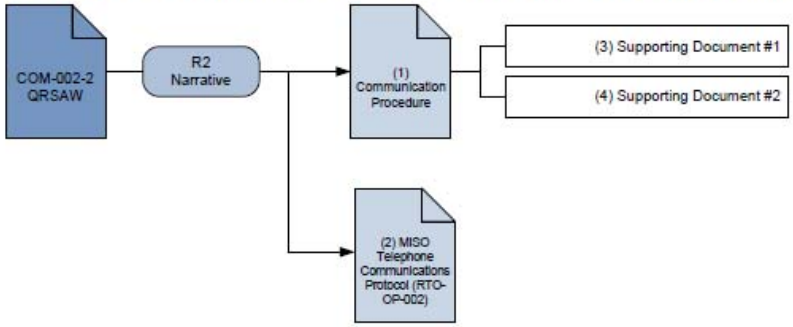
Preparation

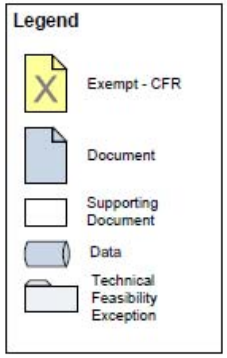
Standard Owner Meeting	Standard Owner Meeting	Internal RSAW Review	Compliance Evidence Review	Standard Owner Meeting	Mock Audit	On-Site Audit
15 months	9 months	8 months	5 months	2 months	1 month	

minnesota power
AN ALLETE COMPANY

Confidential

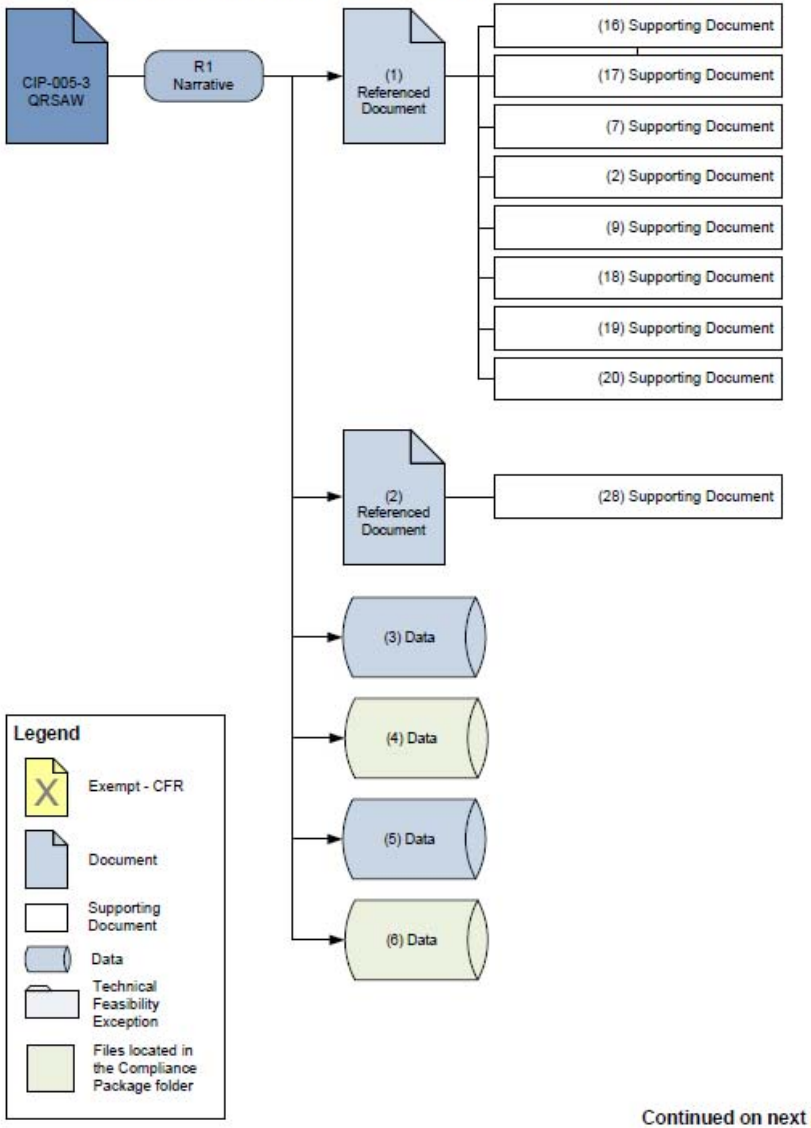
COM-002-2: Communications and Coordination Document Map





Confidential

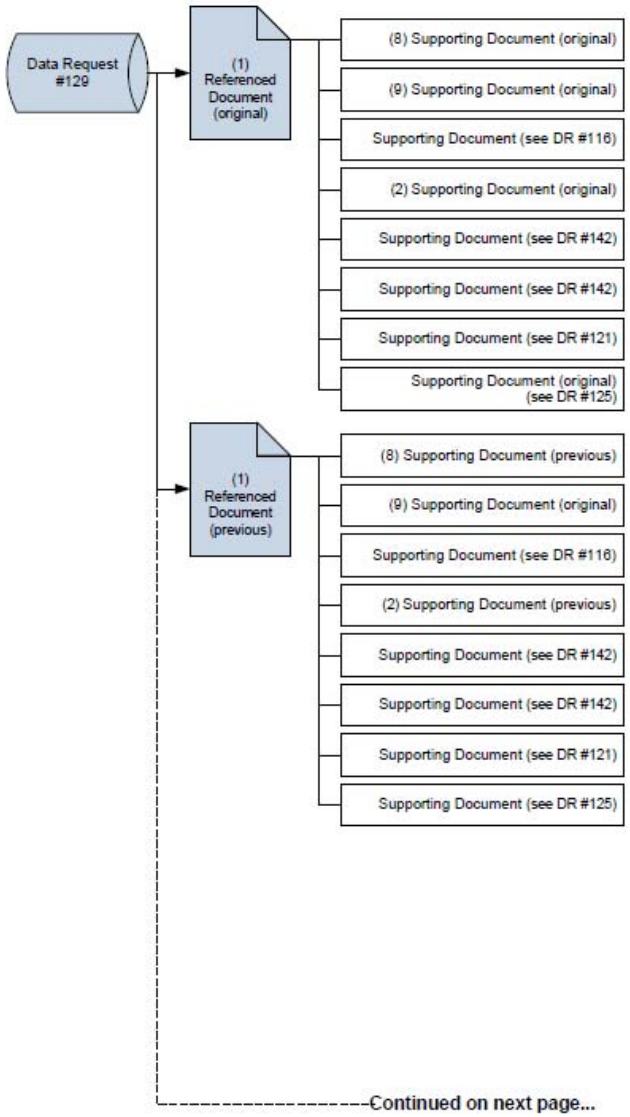
CIP-005-3 Electronic Security Perimeter(s) Document Map



Continued on next page...

Confidential

CIP-005-3 Electronic Security Perimeter(s) Document Map



Continued on next page...

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to COM-002-2 R2.

____Determine if the entity issued directives in a clear, concise, and definitive manner. (No directives were issued during audit period)

____ Determine if the entity ensured that the recipient of the directive repeated the information back correctly. (No directives issued during audit period)

____ Determine if the entity acknowledged the response as correct, or repeated the original statement, to resolve any misunderstandings. . (No directives issued during audit period)

Confidential

« EOP-005 ▸ EOP-005-1 Compliance Package ▸

Search EOP-005-1 Compliance Package

Organize ▾ Burn New folder

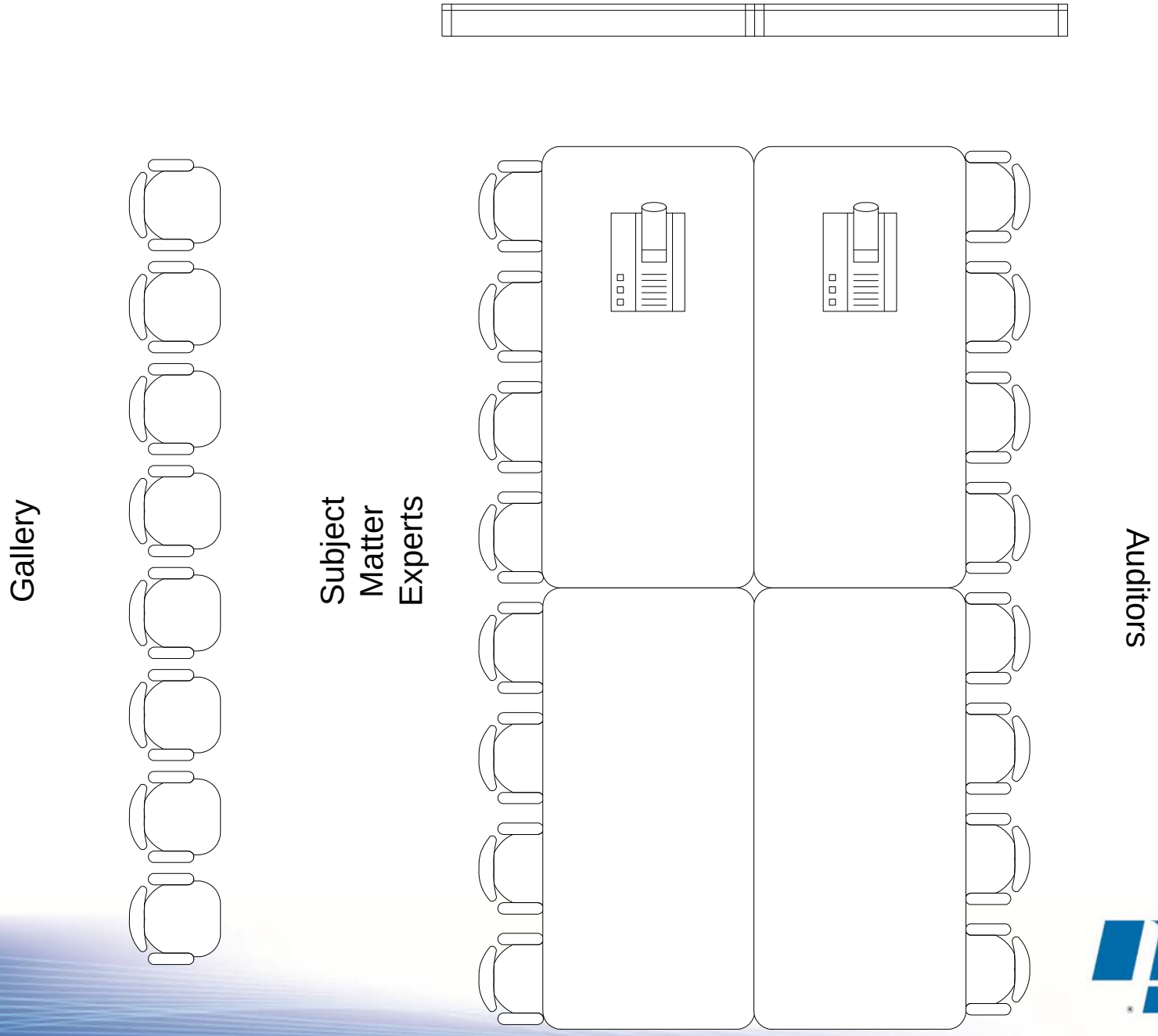
Name	Date modified	Type	Size
(19) Blackstart Test Resu...	8/28/2012 2:43 PM	File folder	
(20) Blackstart Test Resu...	8/28/2012 2:44 PM	File folder	
(1) System Restoration Plan.pdf	6/27/2012 2:57 PM	Adobe Acrobat D...	922 KB
(2) 2009 PSR Course Attendance by Year f...	2/22/2012 5:11 PM	Adobe Acrobat D...	23 KB
(3) 2010 PSR Course Attendance by Year f...	2/22/2012 3:25 PM	Adobe Acrobat D...	25 KB
(4) 2011 PSR Course Attendance by Year f...	2/22/2012 3:26 PM	Adobe Acrobat D...	26 KB
(5) 2012 PSR Course Attendance by Year f...	6/8/2012 1:23 PM	Adobe Acrobat D...	30 KB
(6) Feb 5 2010 Restoration Plan Transmitt...	2/27/2012 2:18 PM	Adobe Acrobat D...	204 KB
(7) Feb 11 2011 MP System Restoration Pl...	2/11/2011 1:51 PM	Microsoft Word 9...	276 KB
(8) Sep 23 2011 MP System Restoration Pl...	10/12/2011 2:28 PM	Microsoft Word 9...	283 KB
(9) May 18 2012 MP System Restoration P...	5/21/2012 3:41 PM	Microsoft Word 9...	275 KB
(10) June 27 2012 MP System Restoration...	7/3/2012 1:38 PM	Microsoft Word 9...	280 KB
(11) 2011 West Emergency Plan Coordina...	10/10/2011 2:36 PM	Microsoft Word D...	136 KB
(12) MP Presentation at MISO EOP-005 W...	7/16/2012 12:42 PM	Adobe Acrobat D...	614 KB
(13) 2009 Training Summary Report by Y...	7/11/2012 10:03 AM	Adobe Acrobat D...	25 KB
(14) 2010 Training Summary Report by Y...	7/11/2012 10:04 AM	Adobe Acrobat D...	25 KB
(15) 2011 Training Summary Report by Y...	7/11/2012 10:04 AM	Adobe Acrobat D...	25 KB
(16) 2012 Training Summary Report by Y...	7/11/2012 10:05 AM	Adobe Acrobat D...	25 KB
(17) NERC Certification System Operators...	6/8/2012 1:38 PM	Adobe Acrobat D...	22 KB

22 items Offline status: Online
Offline availability: Not available

Staffing

- Compliance Department
  - Director, Transmission Regulatory Compliance & Business Support
  - Manager, Compliance and Training
  - Transmission Compliance Specialist, Senior
  - Transmission Compliance Specialist
- Additional Compliance Staff
  - Manager, IT Security and Compliance
  - IT Compliance Specialist, Senior
  - Generation Compliance and Testing Specialist, Senior

Confidential



minnesota power
AN ALLETE COMPANY

Audit Process

- Notice received 90 days prior to the on-site Audit
- Package included:
  - Audit Team
  - Preparing for Compliance Audits
  - Registered Entity Internal Compliance Program Survey
  - Pre-Audit Survey
  - SCADA Network Security Questionnaire
  - Ops & Planning Requests for Information
  - CIP Requests for Information
  - Reliability Standard Audit Worksheets (RSAWs)
  - Audit Team Biographies
  - MRO Audit Certification
  - Standards and Requirements to be Audited

Confidential

Registered Entity Internal Compliance Program Survey

- Describe your internal compliance program
- Identify those responsible for compliance
- Describe the independence of compliance from Operations
- Resources dedicated to compliance
- Self-Audits and Self-Assessments
- Internal Controls

minnesota power
AN ALLETE COMPANY

Pre-Audit Survey

- Organizational Profile
- System Operations
- Registered Functions
- Delegated Reliability Standard Requirements
- Confidentiality and Background Checks
- Travel and Hotel Information

Confidential

SCADA Network Security Questionnaire

- Systems, Protocols and Architecture
- Connections and Features
- Reviews Assessment and Management

minnesota power
AN ALLETE COMPANY

Confidential

Ops & Planning Standards

- BAL-002, R3
- CIP-001, R2, R3
- COM-001, R1, R2
- COM-002, R2
- EOP-001, R3, R7
- EOP-002, R7
- EOP-004, R3
- EOP-005, R2, R4, R6, R10, R11
- EOP-008, R1
- FAC-001, R2
- FAC-002, R1
- FAC-003, R1, R2
- FAC-009, R1, R2
- IRO-004, R1
- IRO-005, R9, R10
- MOD-001, R1, R6
- MOD-004, R3, R4, R6, R8, R9, R10, R11
- MOD-008, R1, R2, R3, R4, R5
- NUC-001, R4
- PER-002, R2, R3
- PRC-001, R1, R2, R3, R4
- PRC-005, R2
- PRC-008, R2
- PRC-017, R1
- TOP-002, R17, R18
- TOP-004, R4
- TOP-007, R3
- TPL-003, R3
- TPL-004, R2

minnesota power
AN ALLETE COMPANY

Ops & Planning RFIs

- 6 Requests related to FAC-003, PRC-005, PRC-008 and PRC-017
- Due 15 calendar days from receipt
- Follow-up Requests were due between 4:30 and 5:00 each day
- 55 Data Requests received and submitted prior to on-site audit

Initial Ops & Planning RFIs

1. A list of all transmission lines 200kV and above in Excel format, including: the line name and the line voltage. (FAC-003)
2. A list of all substations 100kV and above in Excel format, including: the substation name and operating voltages of the substation. (PRC-005)
3. A list of all generating units you own (20 MW and above for single facilities / 75 MW for combined facilities) in Excel format, including: the generator name and generator output. (PRC-005)
4. A list of all UFLS circuits in Excel format, including: the UFLS relay, battery bank, and associated PT. (PRC-008)
5. A list of all SPS circuits Excel format, including the SPS identification, relay, batteries, instrument transformers and communications systems, where appropriate. If any element is owned, or maintained by another entity, provide the name of that entity. (PRC-017)
6. Required completion of the provided spreadsheet, PRC Matrix.xlsx. In addition, provide a copy of the referenced documentation that supports the information provided in the spreadsheet. (PRC-005, PRC-008, PRC-017)

CIP Standards

- CIP-002, R1, R2, R3, R4
- CIP-003, R1, R2, R5, R6
- CIP-004, R1, R2, R3, R4
- CIP-005, R1, R2, R3, R4, R5
- CIP-006, R1, R2, R3, R4, R5, R6, R7, R8
- CIP-007, R1, R2, R3, R4, R5, R6, R7, R8, R9
- CIP-008, R1, R2
- CIP-009, R1, R2, R4, R5

CIP RFIs

- 17 Requests due 15 calendar days from receipt
- 57 Requests due at the time of RSAW submission
- Follow-up Requests were due 24 hours from receipt which was generally between 4:30 and 5:00 each day
- 132 Data Requests received and submitted prior to on-site audit

Initial CIP RFIs

1. A complete listing of ALL BES assets in service during the audit period in Excel format, including: unique identifier, asset name, asset description, function of asset (e.g. transmission substation, generating unit), critical or non-critical, location (street address or GPS coordinates). (CIP-002 R2)
2. A complete listing of ALL cyber assets associated with BES Critical Assets in Excel format, including: asset ID, model, serial #, device type, function the asset supports, technology specifications (e.g. hardware vendor, operating system). (CIP-002 R3)
3. A complete listing of ALL identified Critical Cyber Assets in Excel format, including: asset ID, model, serial #, device type, function the asset supports, technology specifications (e.g. hardware vendor, operating system), Physical location (PSP) where asset resides, logical location (ESP) where asset resides, whether or not the device is dial-up accessible, whether or not each device ties to an active TFE (Yes or No), what TFE number(s), along with associated CIP standard associated to the each TFE, tie to each device (if TFE(s) exist). (CIP-002 R3, CIP-003 R5-R6, CIP-004 R4, CIP-005 R1, R2, R3, CIP-007 R1-R6 and R8, and CIP-009 R4-R5)

Initial CIP RFIs

4. A complete listing of ALL exceptions to the Cyber Security Policy in Excel format, including: unique identifier, Date of exception, Brief description. (CIP-003 R2-R3)
5. A complete listing of ALL access points to all Electronic Security Perimeters (ESPs) in Excel format, including: asset ID, model, serial #, technology specifications (e.g. hardware vendor, operating system), physical location (PSP) where asset resides, logical location (ESP) where asset resides, whether or not the device is dial-up accessible, whether or not each device ties to an active TFE (Yes or No), what TFE number(s), along with the CIP standard associated to each TFE, tie to each device (if TFE(s) exist for the device). (CIP-003 R5-R6, CIP-005 R1-R4, CIP-006 R3, CIP-007 R1, R3-R6, and R8, and CIP-009 R4-R5)
6. A complete listing of ALL devices responsible for monitoring electronic access to Electronic Security Perimeters (ESPs) in Excel format, including: asset ID, model, serial #, technology specifications (e.g. hardware vendor, operating system), physical location (PSP) where asset resides, logical location (ESP) where asset resides, whether or not the device is dial-up accessible, whether or not each device ties to an active TFE (Yes or No), what TFE number(s), along with the CIP standard associated to each TFE, tie to each device (if TFE(s) exist for the device). (CIP-003 R5-R6, CIP-005 R1-R3, R5, CIP-006 R3, CIP-007 R1, R3-R6, and R8, and CIP-009 R4-R5)

Initial CIP RFIs

7. A complete listing of ALL non-critical cyber assets that are located within an identified Electronic Security Perimeter in Excel format, including: asset ID, model, serial #, device type, technology specifications (e.g. hardware vendor, operating system), physical location (PSP) where asset resides, logical location (ESP) where asset resides, whether or not each device ties to an active TFE (Yes or No), what TFE number(s), along with associated CIP standard associated to the each TFE, tie to each device (if TFE(s) exist). (CIP-003 R5-R6, CIP-005 R1-R2, CIP-007 R1, R3-R6, and CIP-009 R4-R5)
8. A complete listing of ALL cyber assets (e.g. servers, workstations, control panels) associated with the system(s) responsible for controlling physical access at each designated PSP in Excel format, including: asset ID, model, serial #, device type, technology specifications (e.g. hardware vendor, operating system), PSP(s) with which the asset is associated, whether or not each device ties to an active TFE (Yes or No), what TFE number(s), along with associated CIP standard associated to the each TFE, tie to each device (if TFE(s) exist). (CIP-003 R5-R6, CIP-005 R2-R3, CIP-006 R2, CIP-007 R1-R8, and CIP-009 R4-R5)

Initial CIP RFIs

9. A complete listing of ALL CIP-related cyber assets (critical or non-critical) that were retired or redeployed during the audit period in Excel format, including: asset ID, model, serial #, device type, status (Retired or Redeployed). (CIP-007 R7)
10. A complete listing of ALL employees and contractors who are currently authorized for unescorted physical access and/or cyber access to Critical Cyber Assets in Excel format, including: employee ID or other unique identifier, individual's full name, individual's company, contractor/employee, position/job title, access status (active/disabled) for each CA or CCA, CA(s) to which unescorted physical access has been authorized and date of authorization/access grant, CCA(s) to which cyber access has been authorized and date of authorization/access grant, date on which access was revoked (if appropriate), whether or not revocation was for cause (if appropriate). (CIP-004 R2-R4)
11. A complete listing of ALL employees and contractors who are currently authorized for unescorted physical access and/or cyber access to Physical Access Control System cyber assets in Excel format, including: employee ID or other unique identifier, individual's full name, individual's company, contractor/employee, position/job title, access status (active/disabled) for each Physical Access Control System cyber asset, Physical Access Control System cyber assets to which unescorted physical access has been authorized and date of authorization/access grant, Physical Access Control System cyber assets to which cyber access has been authorized and date of authorization/access grant, date on which access was revoked (if appropriate), whether or not revocation was for cause (if appropriate). (CIP-004 R3)

Initial CIP RFIs

12. A complete listing of ALL employees and contractors whose unescorted physical access and/or cyber access to Critical Cyber Assets was revoked during the audit period in Excel format, including: employee ID or other unique identifier, individual's full name, individual's company, contractor/employee, position/job title, CA(s) to which unescorted physical access was revoked, CCA(s) to which cyber access was revoked, date on which access was revoked, whether or not revocation was for cause. (CIP-004 R4)
13. A complete listing of ALL designated Physical Security Perimeters (PSPs) that existed during the audit period in Excel format, including: name or other unique identifier, location, associated CA, if any, list of identified Access Points, logs of all reportable incidents associated with this PSP. (CIP-004 R4, CIP-006 R1-R8)
14. A complete listing of ALL outages of physical access control systems for designated Physical Security Perimeters (PSPs) that occurred during the audit period in Excel format, including: outage date, description/summary of outage. (CIP-006 R8)

Initial CIP RFIs

15. A complete listing of ALL tests of the Cyber Security Incident Response plan and actual cyber security incidents that occurred during the audit period in Excel format, including: date of test, event type (test or actual incident), brief description. (CIP-008 R1)
16. A complete listing of ALL cyber security incidents that occurred during the audit period in Excel format, including: unique identifier, date of incident, brief description. (CIP-008 R2)
17. A complete listing of ALL exercises of Critical Cyber Asset recovery plans that occurred during the audit period in Excel format, including: date of exercise, event type (exercise or actual incident), brief description. (CIP-009 R2-R3)
18. 57 Additional RFIs requested completion of the QRSAWs and submission of current and previous versions of policies, plans and procedures. (CIP-002 – CIP-009)
19. For each of the approved TFE, please provide evidence to support the implementation of the compensating measures and ongoing research towards achieving strict compliance as required.

Immediately Before On-Site

- Frequent status update calls with Audit team
- Requests for phone interviews
  - CIP-004, CIP-005, CIP-007
  - PRC-005, PRC-008, PRC-017

On-Site Audit

- Audit Team
  - CIP: 4 MRO Auditors, 1 NERC Observer, 4 FERC Observers
  - Ops & Planning: 4 MRO Auditors, 2 NERC Observers, 4 FERC Observers
- Focus
  - CIP-002, CIP-005, CIP-006, CIP-007
  - Relay Testing, Vegetation Management, and Testing of Customer Owned Equipment

On-Site Audit

- Primary and Backup Control Center Tours
  - Conducted separately
  - System Operator interviews held in the System Operations training room
- Daily Debrief
  - Held a daily debrief with MRO (~4:30 pm)
  - Immediately following we debriefed our SMEs on what we heard (~5:00 pm)

Confidential

Data Request Tracking Sheet

Audit Ops & Planning Data Requests

MRO Data Request	NERC Standard	Requirement	Document Name	Description	Assigned To:	Date Assigned	Due Date	Status	Date Submitted	Form of Submission	Location of Files	Comments
OP-01	FAC-003-1	R2		Implementation of Vegetation Management program; please provide a list of all transmission lines 200kV and above. We request this list to be provided in MS Excel format. Furthermore, for each line segment, we request the Excel spreadsheet include (at a minimum) the following information: the line name and the line voltage. We will use this list to select a sample for R2 to validate the implementation of the annual plan for vegetation management.	Joe Smith	6/28/2012	6/30/2012	Submitted	7/11/2012	EFT Server	P:_Reporting and Responses\Audit\2011_Ops & Planning_Data Requests\OP-01	
OP-02	PRC-005-1	R2		Implementation of Transmission Protection System Maintenance and Testing program; please provide a list of all substations 100kV and above. We request this list to be provided in MS Excel format. Furthermore, for each substation, we request the Excel spreadsheet include (at a minimum) the following information: the substation name and operating voltages of the substation. We will use this list for the evaluation of PRC-005 R2. At a later date, a sample will be selected from the larger population, and additional details will be requested for the selected assets.	John Doe	6/28/2012	7/11/2012	Pending	7/11/2012	EFT Server	P:_Reporting and Responses\Audit\2011_Ops & Planning_Data Requests\OP-02	

minnesota power
AN ALLETE COMPANY

What Happens Next…

- Mitigation & Risk Assessment
  - Work together to develop Mitigation Plans and define milestone activities
  - Can result in a deeper look at the information

Best Practices

- Start **early**
- Get an outside perspective
  - Consultant, internal audit, etc.
- Supervisor involvement
- Documentation Structure
- Space for Auditors and SMEs
- Take advantage of the status calls with auditors before the on-site Audit