Helping our members work together to keep the lights on... today and in the future
Enforcement Process - Evidence
What to Submit, When to Submit, and How to Submit

May 19, 2011

Tasha Ward
Compliance Enforcement Attorney
tward@spp.org / 501.688.1738
Enforcement Process

- Enforcement Process begins with the initial determination of a possible violation

  - Entity Initiated
    - Self-Report
    - Self-Certification (non-compliant)

  - Compliance Staff Initiated
    - Compliance Audit
    - Spot Check
    - Periodic Data Submittal
    - Exception Reporting
    - Compliance Violation Investigation & Complaints
HOW TO SUBMIT EVIDENCE TO ENFORCEMENT

- webCDMS Templates and Forms
  - Self Reports
  - Self Certifications
- Supporting Evidence
  - Additional documentation
  - EFT Server
Data Confidentiality

• Certain information collected during an audit or enforcement activity is highly sensitive and must be protected from inadvertent disclosure

• Examples include:
  – Critical Energy Infrastructure Information (CEII)
  – CIP-protected information
  – Self-report/self certification supporting evidence
  – Mitigation plans supporting evidence
  – Personnel or personally identifying information
Identification of Confidential Information

• **Section 1502, NERC Rules of Procedure**

• The submitting entity shall mark as confidential any information that it submits to NERC or a regional entity that it reasonably believes contains confidential information as defined by the NERC Rules of Procedure.
  
  – Indicate the category or categories defined in *Section 1501* of the NERC Rules of Procedure
  
  – If the information is subject to a prohibition on public disclosure, indicate as such and provide supporting references and details.
Protection of Confidential Information

• NERC Rules of Procedure, Section 1502. Protection of Confidential Information

• “Confidentiality-Except as provided herein, a receiving entity shall keep in confidence and not copy, disclose, or distribute any confidential information or any part thereof without the permission of the submitting entity, except was otherwise legally required.”
Submitting Sensitive Information

- Confidential, sensitive information, such as CIP-protected information should only be submitted via the SPP EFT server
  - Secure HTTP/S connection
  - Automatically PGP-encrypted (AES-256) upon upload to the EFT server
  - Access to encrypted information files limited to SPP RE staff
  - Submitter does not have to have PGP installed
  - If the information is related to an enforcement action, once data is uploaded to EFT server, please send an email notifying the SPP RE Clerk with a copy to the assigned Enforcement case manager
WHAT TO SUBMIT, WHEN TO SUBMIT, HOW TO SUBMIT EVIDENCE TO ENFORCEMENT

Enforcement Process-Evidence:

- Evidence: documentation that supports the entity’s assertions
  - Self Report
  - Self Certification
  - Disagreement of an Initial Determination of a Possible Violation (PV)
  - Mitigation Plan
  - Mitigating factors to the Bulk Power System (BPS)
  - Internal Compliance Program (ICP)
  - Request for Additional Information
Self-Reports

• What to submit
  – Detailed description of the possible violation in webCDMS when submitted to the SPP RE
  – Evidence that the registered entity reviewed in determining that it needed to self-report a possible violation (EFT Server)
    ▪ Examples:
      – Procedure(s)
      – Testing Record(s)

• When to submit
  – When submitting Self-Report
Self Certifications

• What to submit
  – Detailed description of the possible violation in webCDMS
  – Evidence that the registered entity reviewed in determining that it needed to self-certify a standard as non-compliant (EFT Server)
    ▪ Examples:
      – Procedure(s)
      – Testing Record(s)

• When to submit
  – When the registered entity self-certifies as non-compliant
Disagreement with an Initial Determination of PV

• What to submit
  – If entity believes it has evidence to substantiate compliance with the standard, the evidence may submitted to enforcement for review
  – Enforcement will look at the evidence provided and make the subsequent determination of whether or not the additional evidence supports compliance with a standard
  – Burden of proof is for the registered entity to prove by a preponderance of evidence that it was compliant

• When to submit
  – As soon as possible after receiving a Notice of Possible Violation
Mitigation Plans

• What to submit
  – Mitigation Plan submitted in webCDMS
  – Certification of Completed Mitigation Plan - uploaded and submitted in webCDMS
Mitigation Plans

• What to submit
  – Evidence substantiating completion of Mitigation Plan (EFT Server)
  – Remember: if an action is in the Mitigation Plan, evidence must be provided to Enforcement to substantiate completion of the action (e.g. training)
  – Make sure evidence is dated
    ▪ Spreadsheets
      – Created Date
      – Subsequent Revisions
    ▪ Procedures should have revision tables
Mitigation Plans

• When to submit
  – The date the Mitigation Plan is completed
    ▪ If completed early, the registered entity should submit the evidence of completion and Certification of Mitigation Plan Completion at that time
    ▪ No later than the completion date on the Mitigation Plan
    ▪ Compliance Monitoring and Enforcement Program (CMEP) Section 6.6
Mitigating Factors to BPS

• What to submit
  – Evidence supporting mitigation of the risk of the violation to the BPS, should be submitted to Enforcement
    ▪ E.g. If an entity has a violation of PRC-005-1 R1 (lacking or no procedure) yet the entity has been testing its protection system devices (PRC-005-1 R2), entity may submit testing evidence.
Mitigating Factors to BPS

• When to submit
  – As soon as possible
Internal Compliance Program

• What to submit
  – Entity’s documented Internal Compliance Program (ICP)
  – Description of how entity is applying ICP
  – ICP should have an up-to-date revision table
  – Delegated Compliance Responsibility

• When to submit
  – When submitting a self-report or self-certification
  – Other cases: As soon as possible
  – Entity may update the ICP questionnaire
Request for Additional Information

• What to submit
  – Request for Additional Information sent by Enforcement staff or SPP RE File Clerk
  – Enforcement may need additional evidence
    ▪ to determine the full scope of the violation
    ▪ to fully develop and understand the risk to the BPS
    ▪ to verify completion of a Mitigation Plan
    ▪ to determine Violation Severity Level (VSL) Determination
    ▪ to determine if registered entity has affiliates

• When to submit
  – As soon as possible, but no later than due date
Summary

• WHAT TO SUBMIT AND HOW TO SUBMIT

  • webCDMS Templates and Forms
    – In webCDMS

  • Supporting documentation to support assertions
    – EFT Server
    – Send the SPP RE File Clerk an email and copy the Enforcement Case Manager
Summary

• WHEN TO SUBMIT
  – As soon as possible
  – At the time entity submits Self-Report or Self-Certification
  – When the entity has completed its Mitigation Plan
  – No later than the submission deadlines
Questions
Contacts

Manager of Enforcement and Legal
Joe Gertsch  jgertsch@spp.org  501-688-1672

Compliance Enforcement Attorneys/Case Managers
Tasha Ward  tward@spp.org  501-688-1738
Jimmy Cline  jcline@spp.org  501-688-1759
Clay Layson  clayson@spp.org  501-688-1762
Tyler Morgan  tmorgan@spp.org  501-614-3521

SPP RE File Clerk
File Clerk Email  SPPREFileClerk@spp.org
Machelle Smith  msmith@spp.org  501-688-1681