

# Morgan Lewis

## 2011 Edison Electric Institute Fall Legal Conference

Stephen M. Spina  
October 14, 2011



[www.morganlewis.com](http://www.morganlewis.com)

# Overview

- CANs vs. Requests for Interpretation
- Cyber Security (CIP) Compliance
- Relay Maintenance and Testing
- NERC's proposed "Find and Fix" proposal
- NERC Alerts

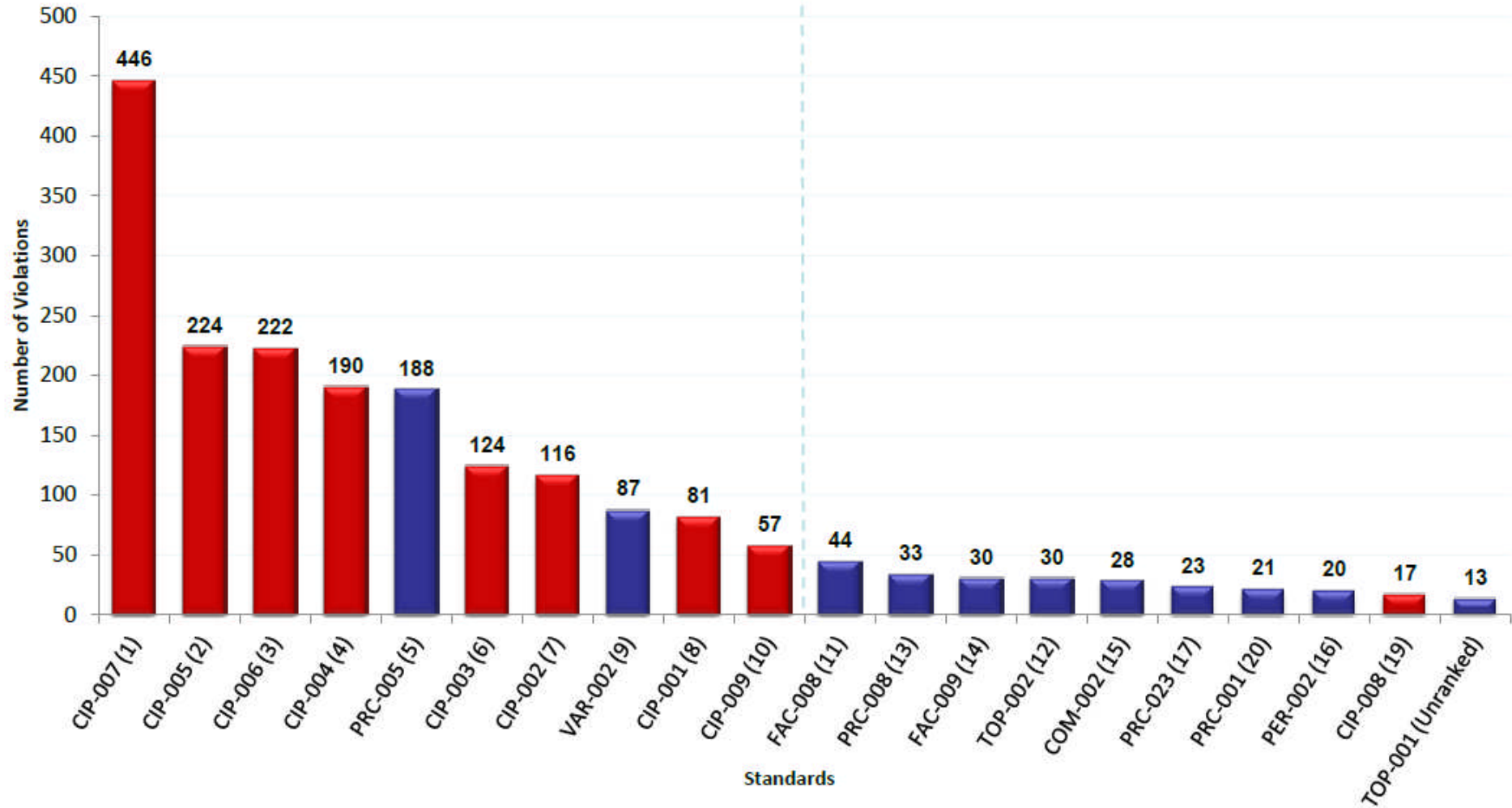
# Compliance Application Notices vs. Requests for Interpretation

- Requests for Interpretation
  - Advantages
    - Can be requested by any entity affected by a Standard
    - NERC is required to respond
    - Comment process includes response to stakeholder comments
    - Must be approved by stakeholder ballot
  - Concerns
    - Very slow development and approval process, delaying guidance on critical compliance issues

# Compliance Application Notices vs. Requests for Interpretation

- Compliance Application Notices
  - Advantages
    - Process developed by NERC in response to industry feedback
    - Faster than interpretation process, providing guidance on emerging issues
    - Provides a limited “notice and comment process” during development
    - Requires FERC approval
  - Concerns
    - No Rules of Procedure process in place to guide development
    - Not “enforceable,” but play a significant role in enforcement
    - Not developed through stakeholder process or voted on by stakeholders
- Problem:
  - CAN process is circumventing Requests for Interpretation, and in many cases, rewriting existing Reliability Standards.

## Previous 12 Months Violations Through August 31, 2011



Analysis Complete: PRC-005, CIP-004, FAC-008, FAC-009, CIP-001, VAR-002, PER-002, CIP-006, CIP-007, EOP-005

# Cyber Security Trends

- Eight of top ten violations are CIP Reliability Standards.
- Approximately 60 percent of violations since June 2010 have been CIP-related violations.
- The total number of Technical Feasibility Exceptions (TFEs) requests that were in the initial stages of the review process as of June 30, 2011, is 5,288.
- The total aggregate number of TFE requests that have been accepted since the process was initiated on January 1, 2010 is 3,492.
- The majority of TFEs relate to the inability to install malware prevention and anti-virus software.

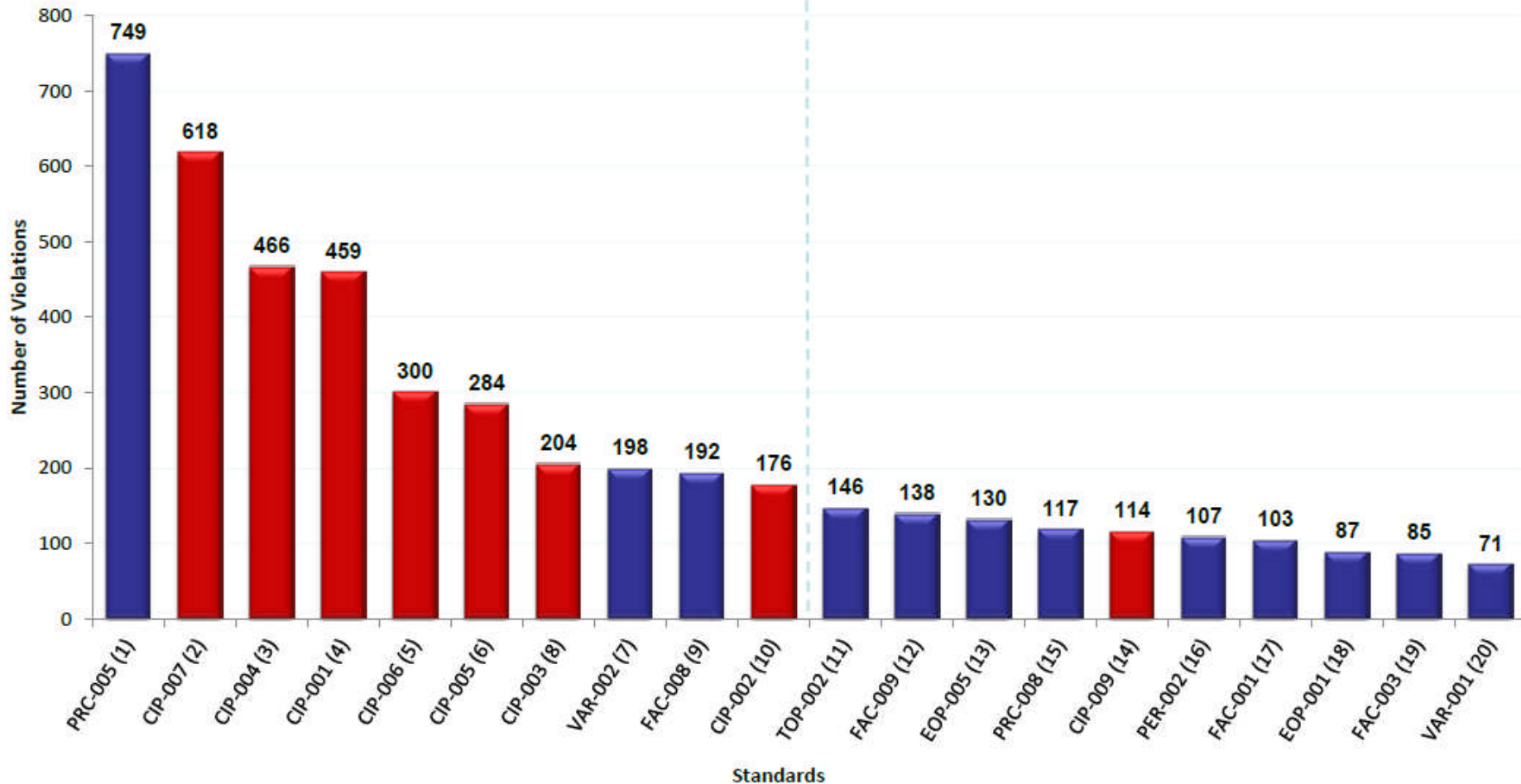
# Cyber Security – Are We More Secure?

- Current CIP Standards set up “walls” to create a secure environment.
  - Electronic Security Perimeter
  - Physical Security Perimeter
- CIP sets minimum level of security performance
- But not much is done to assess what goes on behind the wall. How are companies assessing vulnerability?
  - Few companies are regularly monitoring for vulnerabilities and reporting up in the organization.

# Cyber Security – Are We More Secure?

- Recent industry survey found that few companies have hired people with cyber security backgrounds. Many companies gave IT staff new CIP responsibilities.
- The same industry survey found that companies spend more on TFEs than on incident response.
  - \$123,000 per TFE versus \$119,000 per incident.
- What does this mean?
  - Companies are so focused on the CIP compliance paperwork and preparing for CIP audits, that the crucial work necessary to detect intrusions and identify vulnerabilities is deferred.
  - Compliance with the CIP standards might not prevent a Stuxnet-like attack.

## All-Time Violations Through August 31, 2011



Analysis Complete: PRC-005, CIP-004, FAC-008, FAC-009, CIP-001, VAR-002, PER-002, CIP-006, CIP-007, EOP-005

# PRC-005: Relay Maintenance

- PRC-005 is all-time most violated Reliability Standard.
- The standard requires that entities develop a relay maintenance and testing program with defined testing intervals.
- The standard also requires evidence that the testing and maintenance intervals have been met.
- CAN-008 requires auditors to demand evidence of relay maintenance and testing before June 18, 2007 (the date standards became mandatory and enforceable).
- Entities are scrambling to find evidence of testing before the standards were mandatory.

# PRC-005: Relay Maintenance

- For many entities, testing was performed but records of the testing were not kept because no requirement to do so.
- What is the purpose of this approach?
  - NERC has identified relay maintenance and testing as a top priority.
  - NERC focus on evidence from past periods detracts from effort to make sure programs are strong going forward.
  - Too much time spent on the paperwork hinders effort to ensure that strong programs are in place.

# “Find and Fix” Proposal

- Regions do not have discretion to dismiss minor violations, so detailed records and settlements are required.
- NERC has taken steps to try and relieve the burden. However, even with Administrative Citation Process (ACP), outstanding violations are not decreasing.
- ACP is a backend remedy – does not deal with paperwork and administrative burden placed on entities.
- NERC and regions need discretion on how to deal with violations.

# NERC Filing

- Commissioner LaFleur has stated that “if everything is a priority than nothing is a priority.”
- NERC and the Regions need to assess risk and apply enforcement discretion.
- NERC has tried to address the issue with its Find, Fix Track and Report (FFT) proposal.
- NERC filed with FERC on September 30 and comments are due on October 21.
- This may be a step in the right direction but the key is for the program to reduce paperwork burden on the front end.

# NERC Alerts and Requests for Information

- NERC may use two other functions to require certain actions of users, owners, and operators of the bulk-power system
  - NERC Alerts (Section 810 of the RoP)
    - Three levels: Advisories, Recommendations, and Essential Actions
    - Registered Entities have an obligation to explain their responses to the alerts
      - Can require extensive and expensive actions (e.g. FAC-009 Alert)
    - Only require notification to FERC
    - Only Essential Actions require BoT approval
    - No appeal to FERC available
  - NERC Requests for Information (Section 1600 of the RoP)
    - Requires prior public notice and comment and BoT approval
    - Appeals to FERC available
    - Does not require actions other than supplying the requested information
    - Rarely used by NERC

# NERC Alerts

- Are NERC Alerts becoming *de facto* standards?
- The ultimate cost of response to “Recommendation to Industry, Consideration of Actual Field Conditions in Determination of Facility Ratings” will be considerable.
- No standard was developed and no industry input was sought. Instead, NERC Alert required actions that are significant.
- Like CANs, NERC Alerts are being used to create new and costly requirements without industry input.