Morgan Lewis

NERC Cybersecurity Compliance

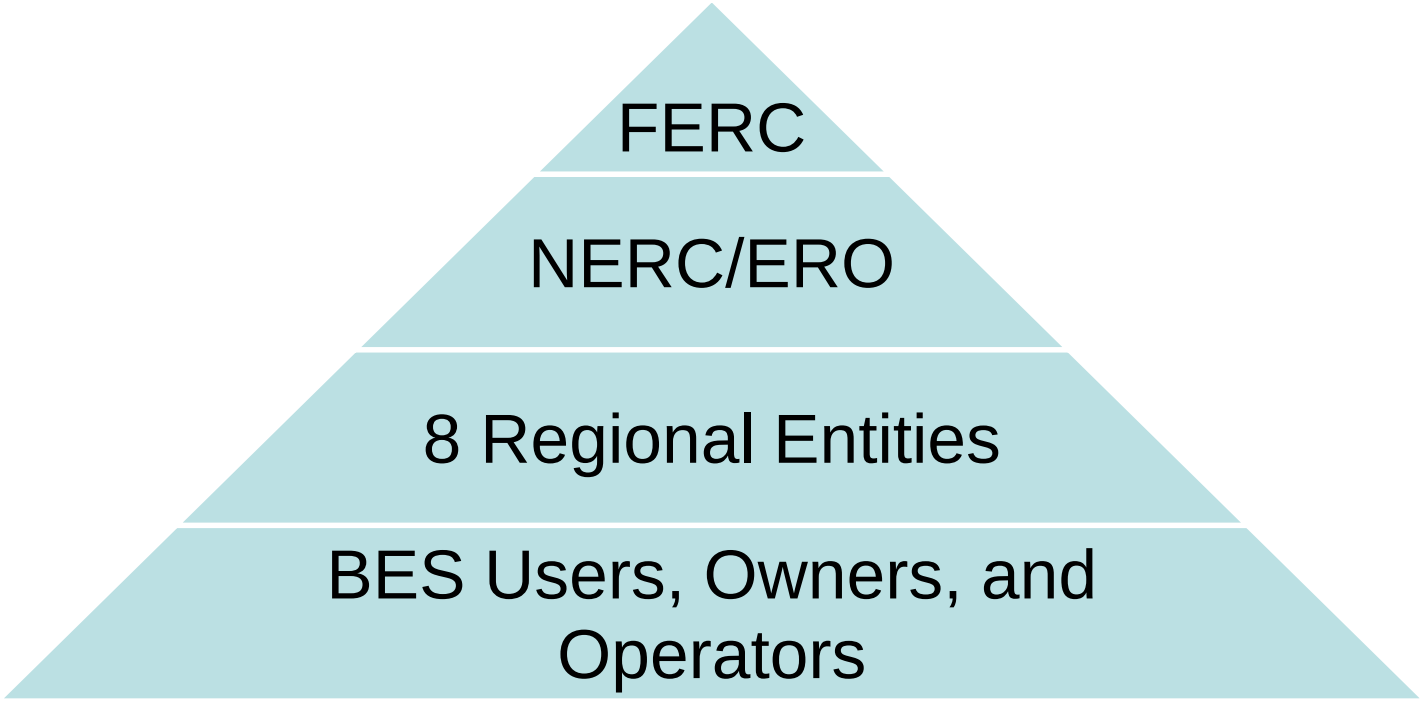
Stephen M. Spina
February 26, 2013

Cyber Attacks on Energy Infrastructure Continue

- According to DHS, the energy sector was the focus of 40% of the reported cyberattacks on critical infrastructure networks in the last fiscal year.
- An attack on a Saudi Arabian oil company last summer wiped data from 30,000 computers.
- Two generators recently reported to have suffered cyber attacks; one knocked the plant out for three weeks.
  1. In one case, “sophisticated malware” was found on two engineering workstations used for operating the control systems.
  2. In another, a technician “carried” the malware and infected the turbine control systems.
     - Used a USB-drive to upload software updates during a scheduled outage for equipment upgrades. Unknown to the technician, the USB-drive was infected with crimeware.

Reliability Structure

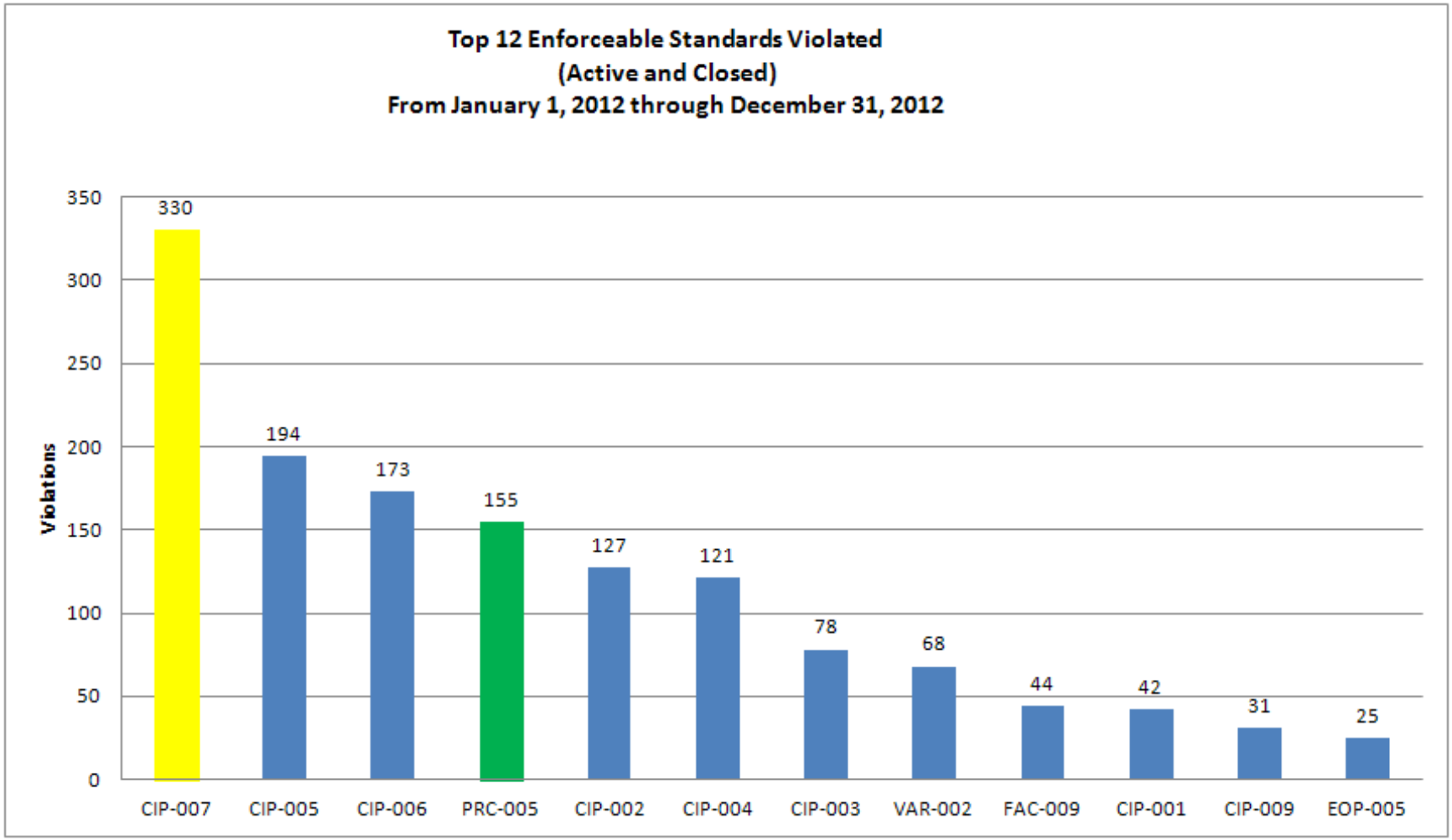
- Section 215 of the Federal Power Act created a three-tiered structure for Reliability Standards development and enforcement, including CIP Reliability Standards.



CIP Compliance and Why It Is Important

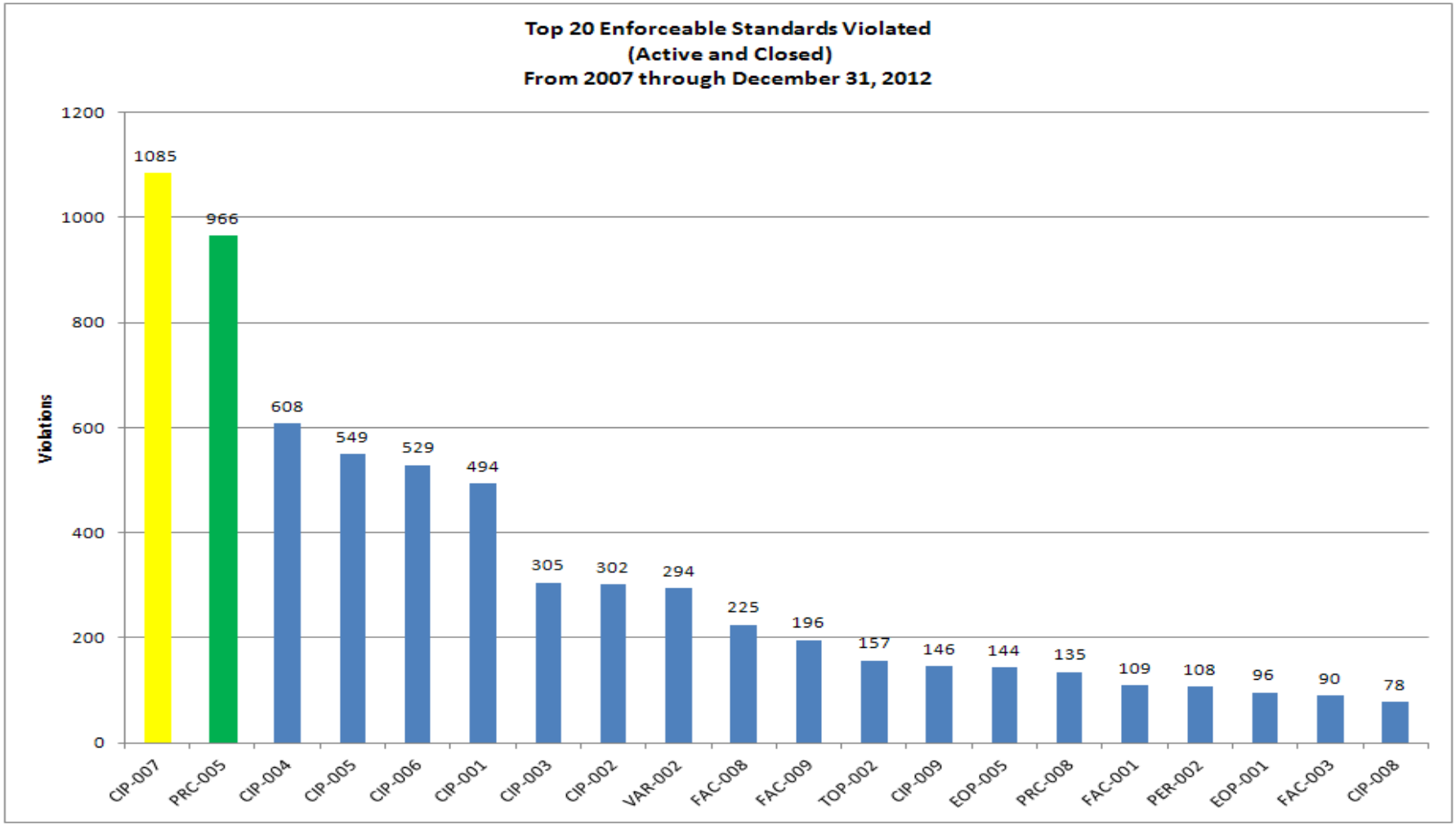
- Importance to utilities:
  - Easy to violate, perfect compliance very difficult
    - A significant human element, regardless of automation
    - Many specific operational and documentation requirements
  - Violations carry heavy penalties: up to $1M per violation, per day as a violation of Part II of the Federal Power Act
  - Provides important security protections for valuable and hard-to-replace assets
- Importance to regulators:
  - Major source of concern for FERC (OER and OEIS)
  - Significant Congressional scrutiny, possibility of legislation
  - Executive concern, as evident in executive order

CIP Standards Violation History



Morgan Lewis

CIP Standards Violation History



Morgan Lewis

History of CIP Reliability Standards

- CIP Reliability Standards address the cyber and physical protection of "Critical Cyber Assets."
  - Version 1 Standards approved by FERC in Order No. 706 in January 2008.
  - Versions 2 and 3 made minor corrections and improvements to address concerns identified by FERC, Version 3 now in effect.
  - Version 4 introduces "bright-line" criteria for identifying protected assets.
  - Version 5 proposal filed with FERC on January 31, 2013. FERC has yet to act on proposal, but is likely to approve it. Version 5 significantly revises the scope of the CIP Standards and the level of protection applied to protected assets.

CIP Version 3—The Standards Today

- First Step: Identify your Critical Assets: “Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”
  - Responsible Entity develops its own risk-based assessment methodology for identifying Critical Assets.
    - E.g., control centers, substations, generators, etc.
    - In practice, FERC/NERC concerned that this leads to under-identification of Critical Assets.
  - Based on that list of Critical Assets, the Responsible Entity then identifies its Cyber Assets that are “essential to the operation” of its Critical Assets and are therefore “Critical Cyber Assets.”
    - Cyber Assets are “Programmable electronic devices and communication networks including hardware, software, and data.”

How to Identify Critical Cyber Assets

- NERC's "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" recommends the following process:
  1) Identify those Cyber Assets associated with a Critical Asset.
     - All Cyber Assets that could impact the reliable operation of a Critical Asset.
  2) Group the Cyber Assets based on shared characteristics that are known to impact the reliable operation of Critical Assets.
  3) Determine which Cyber Assets are "essential."
  4) Determine if those Cyber Assets have qualifying connectivity.
  5) Compile the list of Critical Cyber Assets which receive the stated protections under CIP-003 through CIP-009.

The Compliance Obligations for Identified Critical Cyber Assets

- Second Step: Apply the CIP-003 through CIP-009 protections to all identified Critical Cyber Assets.
- Protected assets include:
  - Critical Assets themselves
  - All Cyber Assets within an identified Electronic Security Perimeter around the Critical Cyber Assets
  - All Cyber Assets used in access control and monitoring of the Electric Security Perimeter and Physical Security Perimeter

CIP Compliance Strategies from the Field

- Establish a stand-alone security organization
  - Separate from compliance, but working with compliance
  - Security expertise; not simply IT expertise
  - Often part of the corporate security organization
- Make the investments that are necessary to achieve compliance
  - In most cases, if you are not CIP compliant you likely have a security gap that could jeopardize costly assets.
    - Mitigation, compliance, and legal costs can also be significant if a violation occurs.
  - Decision-makers need to recognize risks to their assets and operations.
  - State regulators need to understand the risk and the prudence of expenditures to mitigate that risk (NARUC is leading in this area).
    - Replacing an access control and authorization system is cheaper than replacing a turbine destroyed through an Aurora-style attack.

CIP Compliance Strategy: Strong Process Controls

- The Problem: CIP Standards are highly detailed and require the careful implementation of complex procedures. You are held to your procedures.
  - There is always a human component, which leads to human error.
  - There are many individuals who have a role in CIP compliance; an error by a single one can create a compliance violation.
- The Solution: Implement strict process controls to reduce the likelihood of noncompliance.
  - Increase reliance on automation and technical controls, where possible, and reduce reliance on procedural controls.
  - Automated controls fail, but not as often as procedural (i.e. human) controls.

CIP Compliance Strategy: Understanding Compliance vs. Security

- Distinguish between cybersecurity compliance and cybersecurity.
  - Cybersecurity compliance: What is necessary to meet your legal obligations under the CIP Reliability Standards.
  - Cybersecurity: What is necessary to protect your utility assets.
  - The regulatory requirements and business interests have the same objective, but are not equivalent.
- Implement those measures necessary to achieve CIP compliance and define these in your CIP program.

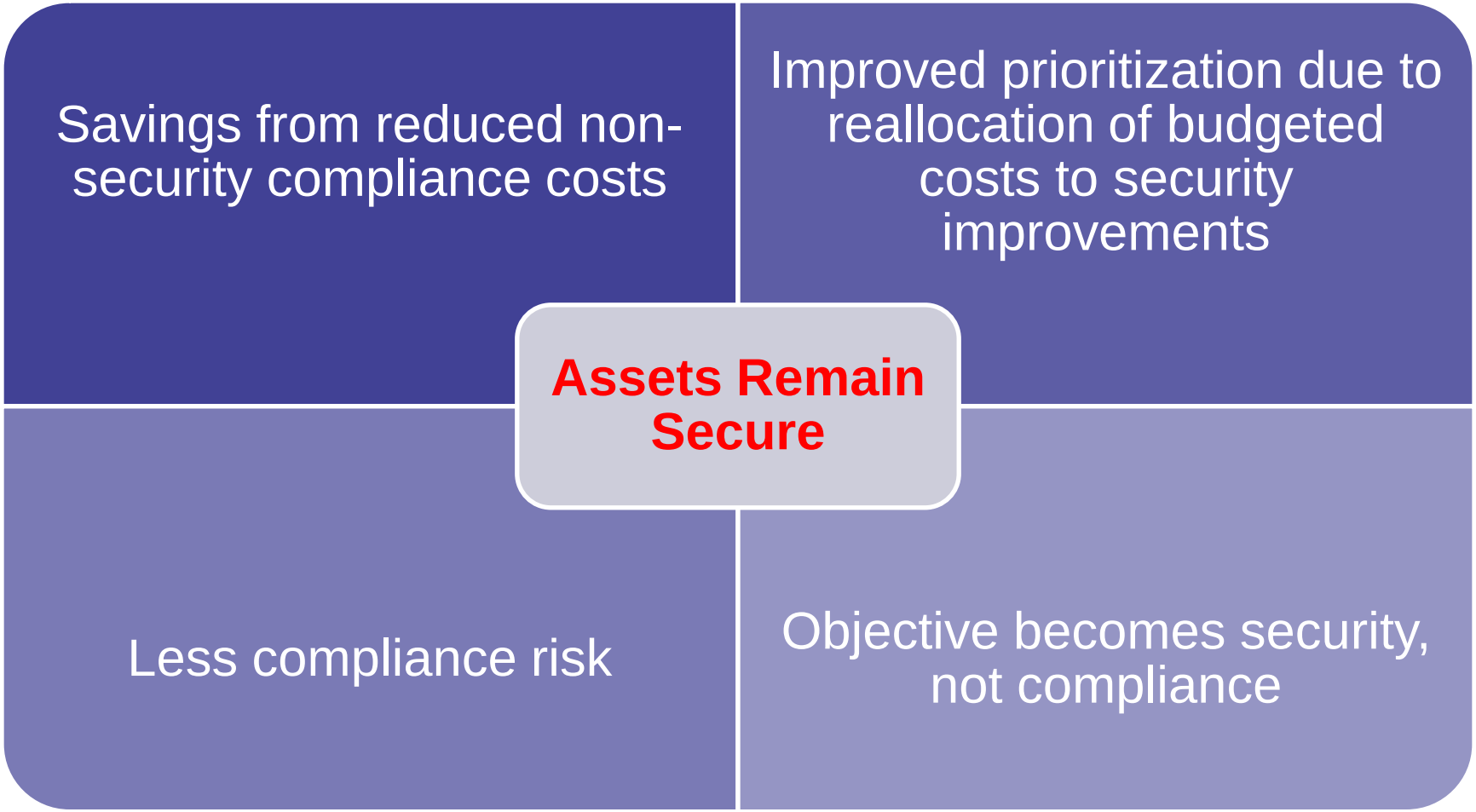
  =The floor for your cybersecurity efforts.
- Implement those measures necessary to achieve security, but not as part of your CIP program.

  =The ceiling for your cybersecurity efforts.

Compliant Is Not Secure

- The intent to go “above and beyond” in setting compliance goals is laudable, because the intent is to improve the security of critical assets.
  - However, from a legal perspective, making these efforts part of the CIP program can create unnecessary risk.
- Need to draw a critical distinction between CIP compliance and the security of your critical assets.
  - CIP compliance should be what you must do to avoid regulatory fines, but often includes what you voluntarily do as well.
  - Security is what you choose to do to protect your assets.

Benefits of Distinguishing Between Compliance and Security



CIP Version 4: The Bright Lines that May Never Exist

- CIP Version 4 removes the risk-based assessment methodology for identifying Critical Assets.
  - Effective April 1, 2014 (i.e. you have until April 1, 2014 to bring assets newly captured by the bright lines into compliance)
- "Bright-line" criteria replaces entity's own determination.
  - Led to inconsistency, perceived under-identification of assets, and concern at FERC and Congress
- If an entity owns or operates an asset that falls within one of the bright-line criteria, that asset is *per se* a Critical Asset.
- HOWEVER, Responsible Entity is still responsible for identifying any associated Critical Cyber Assets based on the same process in CIP Version 1 through 3.

Key CIP Version 4 Bright Lines

- Group of generating units at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.
  - This captures a group of generating units occupying a “defined physical footprint.” These units often have
    - Common fence
    - Common entry point
    - Shared common facilities (warehouses, water plants, etc.)
    - Follow a similar naming convention (plant name-unit number)
    - Fall under a common management organization
    - BUT need not have any of these characteristics

Key CIP Version 4 Bright Lines

- Generating units have a further limitation: the only Cyber Assets that must be considered as potential Critical Cyber Assets are Cyber Assets that:
  1. Within 15 minutes would
  2. Adversely impact the reliable operation of any combination of units at or above 1500 MW
  = If the generating units are separately operated and share no cyber "common mode vulnerability," they would not have any Critical Cyber Assets.
- Control centers for generators meeting the 1500 MW criterion are also *per se* Critical Assets.
  - 1500 MW made up of all controlled generation within a single interconnection.

Key CIP Version 4 Bright Lines

- "Blackstart Resources" identified in the Transmission Operator's EOP-005 restoration plan are Critical Assets.
  - Not simply a generator with blackstart capability
  - Only those generators that are identified in the formal restoration plan
- "Cranking Paths" identified in Transmission Operator's restoration plan are Critical Assets.
  - From the Blackstart Resource to the interconnection point of the generation to be started
  - BUT further limited to the portion of the Cranking Path from the Blackstart Resource up to the point where two or more possible paths exist to the unit to be started

Key CIP Version 4 Bright Lines

- Transmission Facilities:
  - 500 kV or above
  - 300 kV or above at substations with three or more 300 kV+ interconnections with other substations
  - Generator interconnection facilities for generator Critical Assets
  - Transmission facilities needed by nuclear generators to meet Nuclear Plant Interface Requirements (i.e. transmission for off-site power)
  - Transmission Operator control centers that control one or more of these transmission facility Critical Assets.
- Note: Other bright lines exists for SPSs, reactive resources, automatic load shedding Flexible AC Transmission Systems, etc.

Version 5: The Key Changes

- CIP Version 5 Standards filed with FERC on January 31, 2013.
- Would make Version 4 obsolete before it is effective.
  - Version 5 is intended to allow entities to transition from Version 3 directly to Version 5, skipping Version 4.
- According to the proposed implementation plan:

Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

- FERC has yet to act on this proposal, will likely be subject to notice and comment rulemaking.

Version 5: The Key Changes

- Categorization of “BES Cyber Systems” that could affect BES reliability and protection of those systems.
  - No more Critical Cyber Assets.
  - BES Cyber Systems are essentially groups of Critical Cyber Assets.
    - Allows entities to achieve compliance at the group level, rather than the device level.
    - Could meet malware requirements for the BES Cyber System as a whole without the need to install malware prevention on each individual asset.
  - Provides significant entity discretion: generator plant control system could be considered a BES Cyber System or individual components in plan control system could be considered BES Cyber Systems.

Version 5: The Key Changes

- Identifying BES Cyber System compliance requirements is a two-step process:
  1. Identify BES Cyber Systems for controls centers, substations, generation resources, system restoration facilities, SPSs.
     - By definition, a BES Cyber System must, if misused, adversely affect the reliable operation of the BES within 15 minutes.
     - NERC provides extensive on making this assessment.
       - Look to effects of asset loss on dynamic response, balancing, frequency control, voltage control, constraint management, system monitoring and control, system restoration, situational awareness, and inter-entity coordination.
  2. Classify those BES Cyber Systems as “High Impact,” “Medium Impact,” or “Low Impact.”
     - Note: Every BES Cyber System will have a classification and must therefore receive some level of CIP protection; may capture many assets that would not have been covered under CIP Versions 1 through 4.

Version 5: The Key Changes

- "High Impact Rating" BES Cyber Systems are BES Cyber Systems used by and located at:
  - Reliability Coordinator Control Centers
  - Balancing Authority Control Centers for certain 3000 MW Balancing Authorities and certain special categories
  - Control Centers for Transmission Operators
  - Control Centers for Generator Operators with control of certain critical generation (e.g. 1500 MW in an interconnection)

Version 5: The Key Changes

- "Medium Impact Rating" BES Cyber Systems are BES Cyber Systems used by and located at:
  - 1500 MW generating stations (but only for shared BES Cyber Systems that would affect at least 1500 MW in 15 minutes)
  - 500 kV and above transmission facilities
  - 200 kV to 499 kV transmission facilities at a substation interconnected with at least three other 200 kV+ substations that meet certain criticality requirements
- "Low Impact Rating" BES Cyber Systems are BES Cyber Systems used by and located at other facilities not captured in the High and Medium Impact Rating lists.
  - Note: Would still need to be shown to adversely affect the reliable operation of the BES within 15 minutes.

Version 5: The Key Changes

- Actual CIP protections make important improvements based on NERC and industry past experience, but substantively address the same risks and concerns and impose similar requirements.
- But the level of CIP protections depends on the categorization of the BES Cyber Systems.
  - High Impact BES Cyber Systems receive all protections; Low Impact Cyber Systems receive few protections.
  - Standards now have tables discussing the BES Cyber Systems to which the cybersecurity protections apply.

Version 5 Example

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
Reference to prior version: *CIP-007-4, R2.1 and R2.2*		**Change Description and Justification:** *The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.*	
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.
Reference to prior version: *NEW*		**Change Description and Justification:** *On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.*	

Version 5 Example

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.
Reference to prior version: *CIP-006-4c, R1.6.2*		**Change Description and Justification:** *Added the ability to not do this during CIP Exceptional Circumstances.*	

Version 5: Compliance Flexibility

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- Many Requirements now contain the following introduction:

Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies . . .

- Intended to avoid violations for issues that are identified, analyzed, and immediately corrected
  - Focus on improving security, rather than creating compliance and enforcement paperwork
  - There is an open question on the effects that this will have on compliance in practice.

Self-Reporting: When Is It the Right Call?

- Items to consider when self-reporting:
  - There is no affirmative duty to self-report.
  - Self-reporting is a significant mitigating factor in sanction determinations.
    - BUT failing to self-report is not an aggravating factor.
      - Quick remedial action and documentation of the event and the response is essential.
  - Need to evaluate the level of certainty for the conclusion of a violation.
    - Is it dependent on your interpretation of a Requirement?
    - Has there been a Notice of Penalty regarding a violation of the same Requirement or based on the same facts?
  - How significant is the violation?
- Is the mitigating credit worth it?
- Is it likely to be processed through the “Find, Fix, and Track” process?
- Consider the self-certification conundrum: are you likely to need to self-certify on this Requirement?

Avoid Repeat Violations

- FERC is increasingly scrutinizing repeated violations by the same or affiliated Registered Entities.
- Under the Commission's guidance order, a violation should be considered repetitive if it is:
  - the result of conduct similar to the conduct underlying the previous violation of the same, or a closely-related, Reliability Standard Requirement,
  - the result of conduct addressed in a company's mitigation plan for a prior violation of the same, or a closely-related, Reliability Standard Requirement, or
  - an additional violation of the same Reliability Standard Requirement
- An affiliate's violation can be grounds for a finding of a repeat violation if the prior violation involved:
  - an affiliate operated by the same corporate entity or
  - an affiliate whose reliability compliance activities are conducted by the same corporate entity
- Whether the violations happened in different Regions is irrelevant.
- Violations that are considered "repetitive" are subject to heightened sanctions.

How To Demonstrate a Culture of Compliance for CIP Standards

- Follow the general FERC guidelines on a quality internal compliance program.
- Have a good compliance record.
- Participate in and support CIP initiatives (Standards development, compliance conferences, working groups).
- Work with industry groups on lessons learned issues.
  - Transmission Forum
  - Generator Forum
- Get to know your regulators at the Regional Entities, NERC, and the Commission.
- Reach out to the Office of Energy Infrastructure Security.

How To Demonstrate a Culture of Compliance for CIP Standards

- When your utility experiences a cyber incident, consider reporting it to DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).
  - Can respond to and analyze control system related incidents
  - Can conduct vulnerability and malware analysis
  - Can support forensic investigations onsite
- In response to one of the recent attacks on generators, ICS-CERT:
  - Conducted on-site interviews with relevant personnel, imaged the affected machines, analyzed those images, and identified the malware
  - Issued specific recommendations to the affected utility on antivirus, USB best practices, and the importance of "hot spares" for critical systems

Questions?

- Contact Information:

  Stephen M. Spina
  sspina@morganlewis.com
  202-739-5958