PSCC S5 Working Group

Standard Cybersecurity Requirements for Power System Automation, Protection and Control Systems

- Chair: Steven Kunsman
- Vice-Chair: TW Cease

PSCC S5 Working Group

AGENDA

- Introductions
- Call for quorum
- IEEE Call for Patents/IP
- Approval of Sept WG Minutes
- Roundtable development of Cybersecurity architecture and features and applicability to support NERC CIP Compliance
- Status of Writing Assignments
- Next steps

PSCC S5 Working Group

Members

Call for Quorum

xx of 29

Last Name	First Name	Company	Member or Gue
Anderson	Jay	ComEd	M
Becker	Farel	Siemens	M
Bougie	James	GPT	M
Cease	TW	Consultant	M
Cenxon	Ed	SEL	M
Ding	Xiangyu	S&C Electric	M
Dood	Mike	SEL	M
Falk	Herb	SISCO	M
Formea	James	Eaton	M
Giarratano	Didier	Schnieder	M
Haveron	Shane	Ametek	M
Holstein	Dennis	OCG	M
Huntley	Chris Huntley	SEL	M
Johnson	Anthony	SCE	M
Kanabar	Mital	GE	M
Kunsman	Steve	ABB	M
Lacroix	Marc	EMCREY Canada	M
Lombardo	Jason	S&C Electric	M
Luskind	Yuri	iS5com	M
Mackiewicz	Ralph	Sisco	M
Maragal	Deepak	NYPA	M
Mix	Scott	PNNL	M
Newell	Ryan	TRC	M
Nordell	Dan	Xcel Energy	M
Preuss	Craig	B&V	M
Smith	Brian	SCE	M
Thibodeau	Eric	Gentec	M
Wallace	Nathan	Ampirical	M
Zapata	Harry	Duke	M

Participants have a duty to inform the IEEE

- **Participants shall inform the IEEE (or cause the IEEE to be informed) of the identity of each holder of any potential Essential Patent Claims of which they are personally aware if the claims are owned or controlled by the participant or the entity the participant is from, employed by, or otherwise represents**

- **Participants should inform the IEEE (or cause the IEEE to be informed) of the identity of any other holders of potential Essential Patent Claims**

Early identification of holders of potential Essential Patent Claims is encouraged

Ways to inform IEEE

- **Cause an LOA to be submitted to the IEEE-SA (patcom@ieee.org); or**
- **Provide the chair of this group with the identity of the holder(s) of any and all such claims as soon as possible; or**
- **Speak up now and respond to this Call for Potentially Essential Patents**

If anyone in this meeting is personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance, please respond at this time by providing relevant information to the WG Chair

Other guidelines for IEEE WG meetings

- **All IEEE-SA standards meetings shall be conducted in compliance with all applicable laws, including antitrust and competition laws.**
  - **Don't discuss the interpretation, validity, or essentiality of patents/patent claims.**
  - **Don't discuss specific license rates, terms, or conditions.**
    - Relative costs of different technical approaches that include relative costs of patent licensing terms may be discussed in standards development meetings.
      - **Technical considerations remain the primary focus**
  - **Don't discuss or engage in the fixing of product prices, allocation of customers, or division of sales markets.**
  - **Don't discuss the status or substance of ongoing or threatened litigation.**
  - **Don't be silent if inappropriate topics are discussed … do formally object.**

Slide #3

For more details, see *IEEE-SA Standards Board Operations Manual*, clause 5.3.10 and *Antitrust and Competition Policy: What You Need to Know* at http://standards.ieee.org/develop/policies/antitrust.pdf

Patent-related information

The patent policy and the procedures used to execute that policy are documented in the:

- ***IEEE-SA Standards Board Bylaws***
  (http://standards.ieee.org/develop/policies/bylaws/sect6-7.html#6)
- ***IEEE-SA Standards Board Operations Manual***
  (http://standards.ieee.org/develop/policies/opman/sect6.html#6.3)

Material about the patent policy is available at *http://standards.ieee.org/about/sasb/patcom/materials.html*

If you have questions, contact the IEEE-SA Standards Board Patent Committee Administrator at patcom@ieee.org

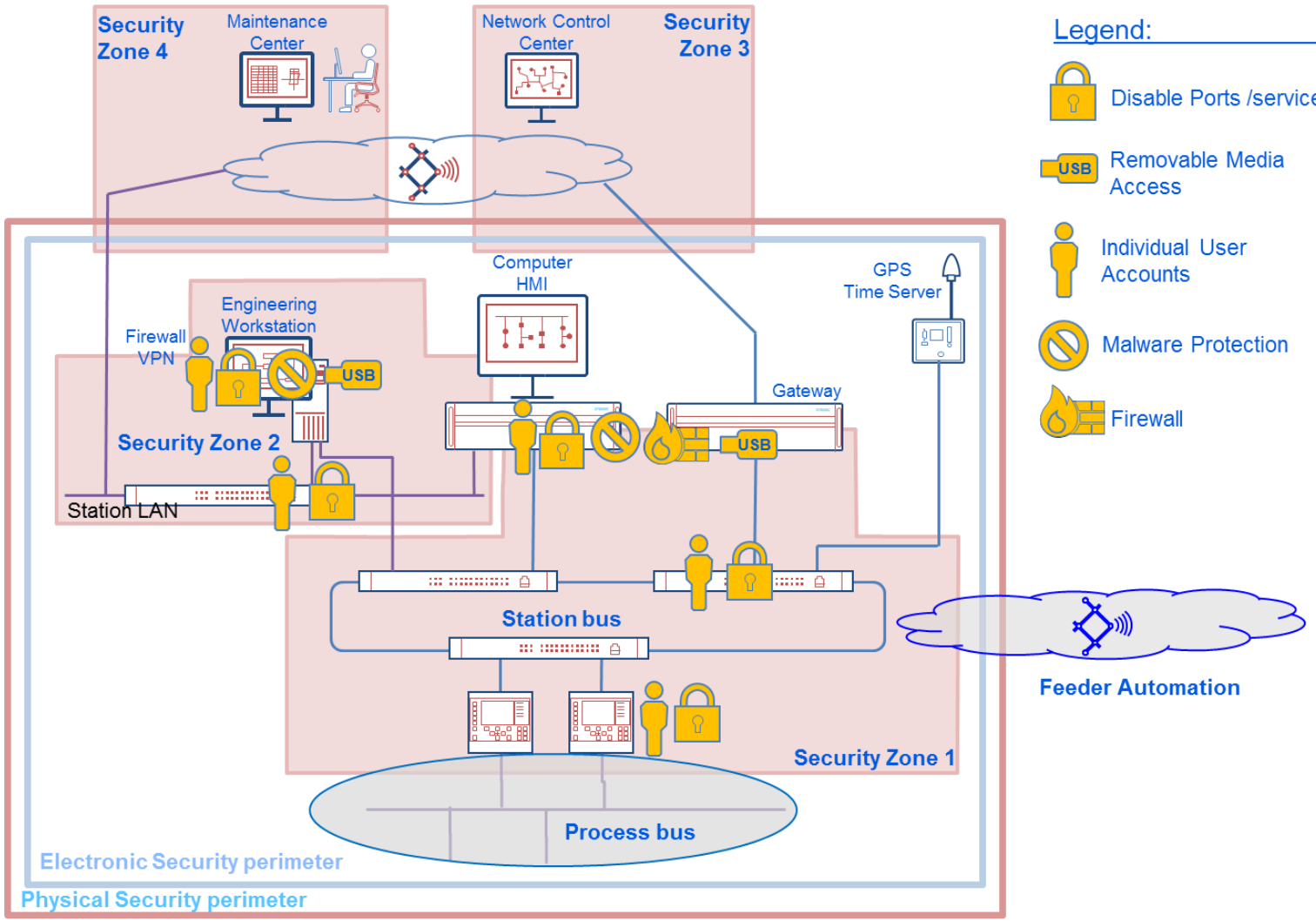
NERC CIP Standards

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-6	Cyber Security - Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security

NERC CIP Standards

- Most of the work will fall into the following NERC CIP Standards:
  - CIP-003 Cyber Security - Security Management Controls
  - CIP-005 Cyber Security - Electronic Security Perimeter(s)
  - CIP-007 Cyber Security - System Security Management
  - CIP-010 Cyber Security - Configuration Change Management and Vulnerability Assessment
  - CIP-011 Cyber Security - Information Protection

Security architecture



Understanding the CIP Requirements

CIP-003-6 — Cyber Security — Security Management Controls

- To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 1 (R1)** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:
- 1.1 For its high impact and medium impact BES Cyber Systems, if any:
- 1.1.1. Personnel and training (CIP-004);
- 1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- 1.1.3. Physical security of BES Cyber Systems (CIP-006);
- 1.1.4. System security management (CIP-007);
- 1.1.5. Incident reporting and response planning (CIP-008);
- 1.1.6. Recovery plans for BES Cyber Systems (CIP-009);
- 1.1.7. Configuration change management and vulnerability assessments (CIP010);
- 1.1.8. Information protection (CIP-011); and
- 1.1.9. Declaring and responding to CIP Exceptional Circumstances.

Understanding the CIP Requirements

CIP-003-6 — Cyber Security — Security Management Controls

- To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 1 (R1)** Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:
- 1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
- 1.2.1. Cyber security awareness;
- 1.2.2. Physical security controls;
- 1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and
- 1.2.4. Cyber Security Incident response
- **Requirement 2 (R2)** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

Understanding the CIP Requirements

CIP-003-6 — Cyber Security — Security Management Controls

- To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 3 (R3)**. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.
- **Requirement 4 (R4)**. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.

Understanding the CIP Requirements

CIP-005-5 — Cyber Security – Electronic Security Perimeter(s)

- To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
- **Requirement 1 (R1)** Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter
  - 1.1 High and Medium Impact **BES Cyber Systems** and their associated PCA: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
  - 1.2 High and Medium Impact BES Cyber Systems with **External Routable Connectivity** and their associated PCA : All External Routable Connectivity must be through an identified Electronic Access Point (EAP).
  - 1.3 **Electronic Access Points** for High and Medium Impact BES Cyber Systems: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
  - 1.4 High and Medium Impact BES Cyber Systems with **Dial-up Connectivity** and their associated PCA - Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.
  - 1.5 Electronic Access Points for **High Impact BES Cyber Systems** and **Medium Impact BES Cyber Systems at Control Centers:** Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.
- **Requirement 2 (R2) E**ach Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management.
  - High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity:
    - 2.1 Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
    - 2.2 Utilize encryption that terminates at an Intermediate System.
    - 2.3 Require multi-factor authentication for all Interactive Remote Access sessions.

Understanding the CIP Requirements

CIP-007-6 — Cyber Security – Systems Security Management

- To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 1 (R1)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*
  - 1.1 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.
  - 1.2 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.
- **Requirement 2 (R2)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.
  - 2.1 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.
  - 2.2 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

Understanding the CIP Requirements

CIP-007-6 — Cyber Security – Systems Security Management

- To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 2 (R2)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*
  - 2.3 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:
    - Apply the applicable patches; or Create a dated mitigation plan; or Revise an existing mitigation plan.

  Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.
  - 2.4 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.
- **Requirement 3 (R3)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R3 – Malicious Code Prevention*
  - 3.1 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Deploy method(s) to deter, detect, or prevent malicious code.
  - 3.2 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Mitigate the threat of detected malicious code.
  - 3.3 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

Understanding the CIP Requirements

CIP-007-6 — Cyber Security – Systems Security Management

- To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 4 (R4)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R1 – Ports and Services*
  - 4.1 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:
    - 4.1.1. Detected successful login attempts
    - 4.1.2. Detected failed access attempts and failed login attempts
    - 4.1.3. Detected malicious code
  - 4.2 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):
    - 4.2.1. Detected malicious code from Part 4.1; and
    - 4.2.2. Detected failure of Part 4.1 event logging.
  - 4.3 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.
  - 4.4 High Impact BES Cyber Systems and their associated EACMS and PCA: Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.
  -

Understanding the CIP Requirements

CIP-007-6 — Cyber Security – Systems Security Management

- To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
- **Requirement 5 (R5)** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R5 – System Access Controls*.
  - 5.1 High Impact BES Cyber Systems, Medium Impact BES Cyber Systems at Control Centers and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA: Have a method(s) to enforce authentication of interactive user access, where technically feasible.
  - 5.2-5.7 High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated EACMS, PACS and PCA:
    - 5.2 Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
    - 5.3 Identify individuals who have authorized access to shared accounts.
    - 5.4 Change known default passwords, per Cyber Asset capability
    - 5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:
    - 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and
    - 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.
    - 5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.
    - 5.7 Where technically feasible, either: 1) Limit the number of unsuccessful authentication attempts; or 2) Generate alerts after a threshold of unsuccessful authentication attempts.

Status of Writing Assignments for IEEE C37.240 revision

- **Cyber security requirements for communications outside the control house but inside the substation fence** – Steve Kunsman, Farel Becker, Herb Falk, Jay Anderson, James Formea
- **H22 Guide for Cyber Security for Protection Related Data Files** – Tony Johnson, TW Cease, Dennis Holstein
- **Cyber security for protection systems outside of the substation** (Feeder automation/Wide area systems) – Ryan Newell, Chris Huntley, Mital Kanabar, Xiangyu Ding, Peter Rietmann
- **Cyber security requirements for wireless applications**. There was an in depth discussion on the wireless topic. There are two aspects to wireless (physical and data) and ISA 100 would be a good starting point to review. The focus should be on How to assess the cybersecurity requirements for wireless. – Craig Preuss, Marc Lacroix, Dennis Holstein
- **Application Whitelisting and Blacklisting** including Communication Whitelisting Herb Falk, Craig Preuss, Mark Lacroix
- **Applications and Management of Digital Signatures** – Herb Falk, James Formea, Didier Giarrantano
- **Cloud based application** – Nathan Wallace, Dennis Holstein
- **C37.240 audit support documentation** (also to review IEC 62443-2.4 for auditing– Tony Johnson, Jay Anderson
- **Reference appendix to map the standard into NERC CIP applications** – Tony Johnson, Scott Mix