RELIABILITY FIRST

Low Impact Focus Group

Monthly Meeting

October 24, 2017






Opening Comments

- **This meeting is being recorded**
- **All lines are open in order to facilitate discussion**
- **Please mute your line when not speaking**
- **Please do not put this call on hold – many systems play music on hold**
  - If you need to answer another call, please disconnect and call back in

Announcements

- **NERC's Antitrust Guidelines are available at:**
  - http://www.nerc.com/pa/Stand/Resources/Documents/NERC_Antitrust_Compliances_Guidelines.pdf
- **This is a public call. RF cannot pre-screen the attendees.**

Mailing List

- ciplifg@lists.rfirst.org
- This list is intended as a discussion forum.
- List changes, such as additions or removals, should be sent to: lew.folkerth@rfirst.org

Survey Results

- Lew conducted an informal on-line survey
- Results are anonymous
- There were 49 survey visits, 43 completed responses, and 2 partial responses

Survey Results

Special Topics	Not Important	Somewhat Important	Important	Score	Rank
Introduction to CIP Low Impact Requirements and Compliance	27.27% 12	22.73% 10	50.00% 22	282	7
Low Impact Electronic Access Controls	0.00% 0	20.45% 9	81.82% 36	405	1
Low Impact Physical Access Controls	4.55% 2	25.00% 11	70.45% 31	367	3
Low Impact Compliance Documentation and Evidence	6.82% 3	13.64% 6	79.55% 35	383	2
Field Experience with Low Impact Implementation (Notes and experiences from a CIPLIFG member)	4.55% 2	34.09% 15	61.36% 27	347	4
What Happens During an Audit?	9.30% 4	32.56% 14	58.14% 25	324	6
In-depth Discussion of Emerging Standards Applicable to Low Impact	11.36% 5	27.27% 12	61.36% 27	335	5

Survey Results

- **Please suggest additional topics:**
  - the key thing for all topics discussed is that RF needs to present only the facts and not speculate on what could or could not be needed for compliance with the Standard. For example, if RF does not know how what the audit expectations are, then the answer is TBD. Providing any speculative answers that go beyond the language of the Standard will create unintended expectations that Registered Entities may expend considerable resources to achieve.

Survey Results

- **Please suggest additional topics:**
  - I'm fairly new to compliance. All the suggested information would be very welcome. Thanks.
  - I am sure they are all important. Those I marked as important should be covered first in my opinion.
  - An IT101 focus might be good for the group. Where I struggle is understanding some of the technical terminology and applying the Standards to the actual equipment we have on site. Example; routable dial up connectivity, DMZ, etc.
  - Discussion relative to the Reference Models in CIP 003

Survey Results

➢ Please suggest additional topics:

- In general, whatever is presented needs to be based on facts and not speculation. There is very little low impact guidance available and any information provided by a regulator should be based on what will be done and not what could be done. Entities need to have a clear understanding of RF expectations in order to provide the proper focus and resources in developing a low impact program. The existing published Attachment C includes a Tab and evidence sampling questions that based on the current and pending Standard language, would not be applicable (i.e. LI Cyber Assets list). RF personnel have indicated this information is not required and optional, however, because it is a regulator published document, entities could interpret this as something RF is expecting to see now or in the future. Being a regulator, only the actual information required and expectations should be published in official documents. If an entity wants to provide something optional, then it should be their choice and not included as part of the primary tool used by RF to audit compliance. This type of miss information could lead an entity to apply significant resources to address an unintended expectation rather than focusing those resources on concerns that have a more significant reliability impact. The same approach should be used by NERC/RF when making any public statements regarding compliance expectations (i.e. facts only and not speculation). In the absence of clear expectations, every word from a regulator can make a difference in how a program is developed.

Survey Results

- **Do the monthly CIPLIFG meetings provide value to your organization?**
  - Yes: 39 (92.9%)
  - No: 3 (7.1%)
- **Should the CIPLIFG monthly meetings be continued?**
  - Yes: 43 (100%)
  - No: 0 (0%)

Survey Results

➢ Additional comments or feedback

- Since I am new to the Compliance side of the business, I appreciate any and all extra information I can learn about the subject. We are a low impact, or even below that level, entity. Thanks in advance for all the time and assistance in this area.
- It seems like this group is slow in starting up. I do believe with the subjects noted in this survey that it should take off and be more vital to an organization. It would also be nice to have the presentation available a few days ahead of time so that entities may review it and note any questions they may have before the meeting or presentation.

Survey Results

➢ Additional comments or feedback

- This group can be a very key part in providing valuable information to the industry on the compliance expectations of RF. There has been a lot of speculation and miss information about what is needed by a Registered Entity to demonstrate compliance for low impact systems (e.g. a published Attachment C with a Low Impact Cyber Asset tab to be used for sampling during an audit.). These monthly meetings could be used to clarify and establish clear expectations based on facts and the language of the Standard. Please continue them!

Survey Results

➢ Additional comments or feedback

- The CIPLIFG has been understandably geared towards entities with no Medium or High-Impact BCS so far. Entities that already have these types of BCS would get more value in discussing types of cyber assets at low impact sites, implementing the reference models from CIP-003-6, and details on what type of evidence will be expected for access (physical keyholder lists? drawings of LEAP/LERC/Physical boundaries, awareness, etc.)

Survey Results

➢ Additional comments or feedback

- Would like to see presentations from entities on how the are implementing their low impact compliance program. In particular any challenges or redesigns involving electronic access controls.

Survey Results

➢ Additional comments or feedback

- may want to reevaluate periodicity to determine if monthly is too frequent.
- Frequency of meetings could probably be stretched to bi-monthly.

Survey Results

➢ Additional comments or feedback

- There is much potential for the meeting and I would like to see it continue.
- We attend as possible.
- None at this time
- no additional requests.
- I would like to say thanks for having this group.
- Thanks for doing this!!!

Survey Results

➢ Key take-aways

- There is significant interest in all suggested topics. Possible additional topics: IT-101 (Intro to information technology and cyber security language and concepts)
- When covering access controls, ensure the CIP-003 reference models are covered.
- Include recommended evidence where possible.
- RF's presentations and documents must clearly differentiate between actions required by a Standard and recommended practice.
- Regular meetings should continue, although possibly on a bi-monthly schedule.

Standards Update

➢ CIP-003-7 NOPR

- FERC issued a Notice of Proposed Rulemaking (NOPR) at its October 19, 2017, open meeting.
- The NOPR is located at: https://www.ferc.gov/whats-new/comm-meet/2017/101917/E-1.pdf.

Standards Update

➢ CIP-003-7 NOPR

- P31,32: Electronic Access Controls
  - "CIP-003-7 does not provide clear, objective criteria or measures to assess compliance by independently confirming that the access control strategy adopted by a responsible entity would reasonably meet the security objective of permitting only 'necessary inbound and outbound electronic access' to its low impact BES Cyber Systems." (P28)
- Four proposed criteria:
  - Electronic access granted through an authorized and monitored electronic access point (CIP-005-5 R1)
  - Electronic access granted based on need (CIP-005-5 R1 Part 1.3)
  - Methods to enforce authentication of users (CIP-007-6 R5)
  - Strong passwords, password change intervals (CIP-007-6 R5)

Standards Update

➢ CIP-003-7 NOPR

- P40,41: Transient Cyber Assets
  - "The proposed Reliability Standard may, therefore, contain a reliability gap where a responsible entity contracts with a third-party but fails to mitigate potential deficiencies discovered in the third-party's malicious code detection and prevention practices prior to a Transient Cyber Asset being connected to a low impact BES Cyber System."
- Two proposed criteria:
  - Mitigate any malicious code found during the third-party review, or
  - Take reasonable steps to mitigate the risks of third party malicious code on their systems, if an arrangement cannot be made for the third-party to do so

Standards Update

➢ CIP-003-7 NOPR

- P45: Effective date
  - "[T]he proposed implementation plan does not alter the previously-approved compliance dates for Reliability Standard CIP-003-6 other than the compliance date for Reliability Standard CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3, which would be replaced with the effective date for proposed Reliability Standard CIP-003-7."
- This appears to mean that the effective date for the requirements for electronic and physical access controls for low impact BES Cyber Systems will slip from September 1, 2018, to October 1, 2019, at the earliest. <u>This is subject to change based on comments to this NOPR.</u>

Future Meetings

- **Next conference call (WebEx):**
  - Tuesday, November 14, 2017 at 11:00AM EDT
  - Determine at that call whether to schedule the December meeting

Future Meetings

➢ Planning for future meetings:

- Presented via WebEx
- Recorded and posted on RF's LIFG site
- Topics in priority order:
  - Low Impact Compliance Documentation and Evidence
    - Part 1 –Requirements Currently in Effect
  - Field Experiences
  - Low Impact Physical Access Controls
  - IT-101: Intro to IT and Cyber Security Terminology
  - CIP-101 for Low Impact: Intro to CIP Requirements, Compliance, and Audits

CIPLIFG Web Site

- **Possible new section: Tools**
- **Free (or inexpensive) tools or information**
  - Vendor neutral
  - Publicly available
  - Industry specific
- **RF CIPC**
  - As discussed on the call, membership in the RF Critical Infrastructure Protection Committee (CIPC) is available to entities registered with RF. Membership information is available in this document: https://www.rfirst.org/cipc/Documents/RF%20CIPC%20Welcome%20Letter.pdf

Questions & Answers

Forward Together **ReliabilityFirst**