2019 DLC

April 1 - 3 • St. Louis, MO

STAKEHOLDER MEETING

2019 DLC April 1 - 3 • St. Louis, MO

STAKEHOLDER MEETING

Cybersecurity Discussion

Levin Nock

DLC

Paul Ayers

DLC

Gabe Arnold

DLC

Bagwat Mohan

DLC

Kurt Nielson

Consultant to DLC

WHO'S HERE?

Agenda:

▪ Expectations / Ground Rules	5 mins
▪ Cybersecurity Introduction	10 mins
▪ Summary of Comments Received	10 mins
▪ Discussion Break-Outs	30 mins
▪ Report Outs	25 mins
▪ Next Steps	5 mins

DO'S

- ✓ Share your perspective
- ✓ Ask Questions!
- ✓ Stay on Topic
- ✓ Write it down!

DON'TS

- × Soapbox
- × Talk Over Others
- × Argue Semantics
- × Throw Tomatoes

[Statler & Waldorf Image] retrieved from URL: http://pointmeister.blogspot.com/2010/01/late-night-with-statler-waldorf.html

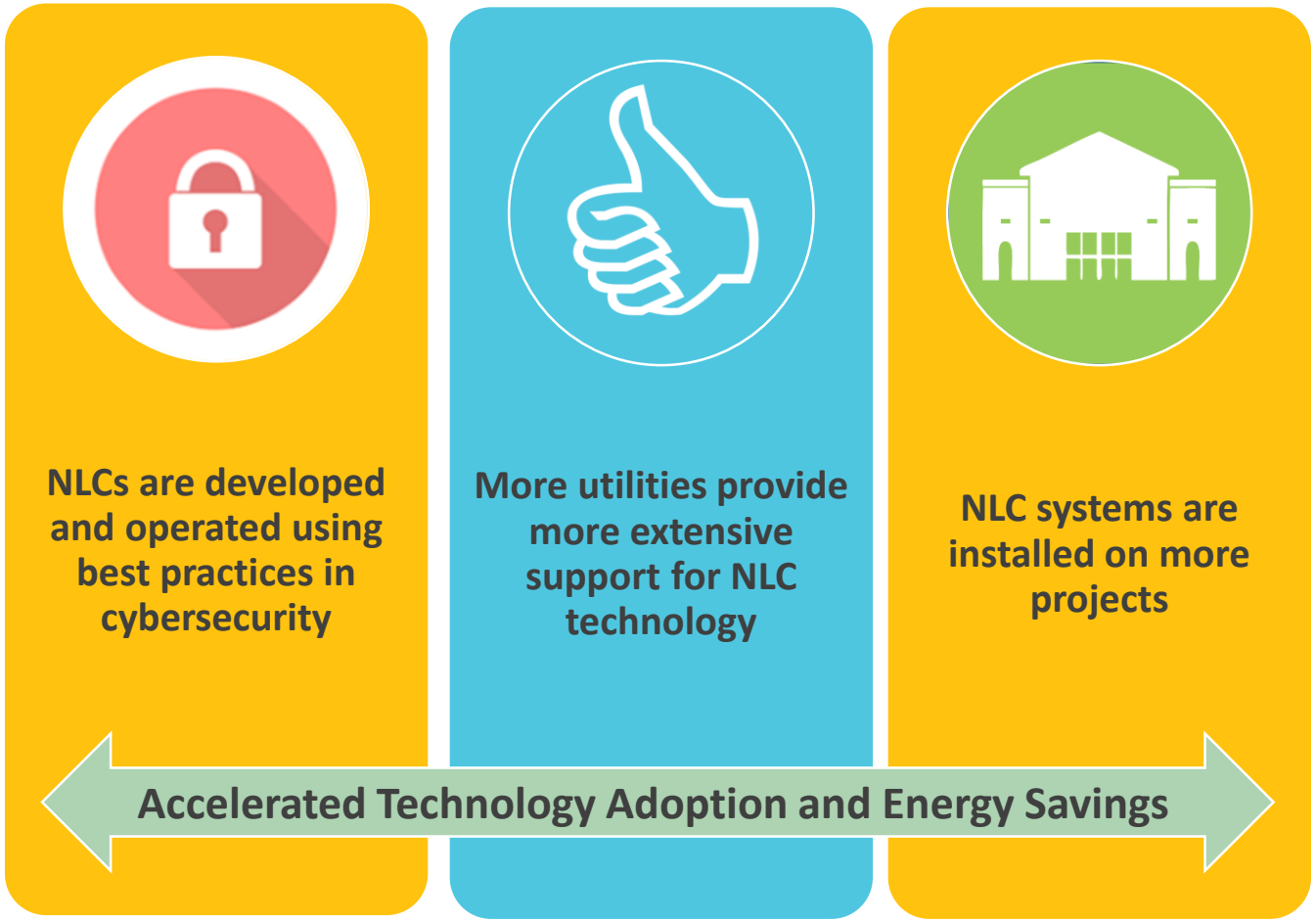
[Statler & Waldorf Image] retrieved from URL: http://pointmeister.blogspot.com/2010/01/late-night-with-statler-waldorf.html

V4.0 Focus Area

Cybersecurity

- The practice of defending networked systems and data from malicious attacks
- Critical for customer trust and adoption

Desired Outcomes



Cybersecurity Plan

June 2018 V3

Cybersecurity activity is reported.

June 2019 V4

Establish criteria to qualify a set of cybersecurity standards.

Only products that comply with a qualified standard may declare the **optional** cybersecurity capability.

June 2020 V5

Cybersecurity is **Required**. Products must comply with at least one standard that meets the criteria defined in V4 (or reapply under V4 with the 1-year grace period).

June 2021 V6

Cybersecurity is **Required**.

Criteria for Acceptable Cybersecurity Standards

1. Certifiable with a standardized methodology established through either:
   - A voluntary consensus process such as ANSI, ISO, IEC…
   - A federal agency of the USA or Canada
2. Multiple third-party accredited labs are available to perform testing and certification
3. Applies to one or more of the following:
   a) Product development process lifecycle
   b) Components
   c) System
   d) Cloud Services
4. Includes at least 3 of the following technical content, for (b,c,d) above
   a) Penetration testing
   b) Communication robustness testing
   c) Vulnerability identification testing
   d) Multiple levels of security

Cybersecurity standards meeting the draft criteria

(updated based on comments)

Standard	Process	Components	System	Cloud Services
ANSI/UL 2900-1	y	y	?	
CTIA (cellular)	y	y		
IEC 62443	-4-1	-4-2	-3-3	
ISO 27001	y			
FedRAMP				y
SOC2	y		y	y
CSA STAR				?
ISO 2017				y

Future potential standards

ANSI/UL 2900-2-4 for BMS; ANSI/UL 2900-2-5 for lighting

CSA T-200 (CVP Cybersecurity Verification Process, BSIMM)

Draft 1 Proposed Timeline

Timeline	Process	Components	System	Cloud Services
V5.0 2020	Required	Required		
V6.0 2021	Required	Required	Required	Required

Agenda:

Expectations / Ground Rules	5 mins
Cybersecurity Introduction	10 mins
Summary of Comments Received	**10 mins**
Discussion Break-Outs	30 mins
Report Outs	25 mins
Next Steps	5 mins

Summary of Comments Received

1. Make the timeline more flexible
2. Fewer requirements if external network is not supported
3. Add or remove standards
4. Revise criteria and terminology

Revised Plan for Draft 2 Timeline

4 Types: Process, Components, System, Cloud

2020: Any one type of cybersecurity certification is required

2021: “Process” certification is required

2022: Further requirements to be determined.

- One possibility would be to require 2 types in 2022, 3 types in 2023, etc.
- Another possibility would be to recognize multiple levels of security, for instance:
  - Level 1: Process audit
  - Level 2: Process audit with limited product testing
  - Level 3: Process audit with extensive testing plus cloud certification

Cybersecurity Discussion Topics

- Topic 1 Exceptions w/o external networking
- Topic 2 Criteria for acceptable standards
- Topic 3 Add or drop standards?

Topic 1: Exceptions w/o external networking

- What exception(s)?
- How to define a system that qualifies for the exception?

Topic 2: Criteria for acceptable standards

- Require consensus?
- Appropriate technical content?
- Are multiple third-party labs necessary?
- Should “Process” address particular details?
- Other changes to the draft criteria?

Topic 3: Add or drop standards?

- Remove from the list?
- Add to the list?
- Clarify the question marks in the table?

Clarifying Questions?

Agenda:

Expectations / Ground Rules	5 mins
Cybersecurity Introduction	10 mins
Summary of Comments Received	10 mins
Discussion Break-Outs	**30 mins**
Report Outs	25 mins
Next Steps	5 mins

Break Out:

Step 1: Pick a Topic that is most relevant to you

Topic 1	Topic 2	Topic 3
Exceptions without External Networking	Criteria for Acceptable Standards	Add or Drop Standards

Step 2: Move to table for that topic (or stay where you are)

Step 3: Review the context and questions

Step 4: Write it all down!

Break Out Guidance:

1. Discuss context and topic among the table

2. Review and discuss the open questions

3. Capture the brainstormed feedback on the flip charts

4. Technical team will be floating to answer questions

Agenda:

Expectations / Ground Rules	5 mins
Cybersecurity Introduction	10 mins
Summary of Comments Received	10 mins
Discussion Break-Outs	30 mins
Report Outs	**25 mins**
Next Steps	5 mins

Table Report Out Format

1. What Topic did you investigate? 1 min

2. What are 2-3 Key Take-Aways? 2 mins

Report Out:

Topic 1	Topic 2	Topic 3
Exceptions without External Networking	Criteria for Acceptable Standards	Add or Drop Standards

Report Out:

Topic 1	Topic 2	Topic 3
Exceptions without External Networking	Criteria for Acceptable Standards	Add or Drop Standards

Report Out:

Topic 1	Topic 2	Topic 3
Exceptions without External Networking	Criteria for Acceptable Standards	Add or Drop Standards

Agenda:

▪ Expectations / Ground Rules	5 mins
▪ Cybersecurity Introduction	10 mins
▪ Summary of Comments Received	10 mins
▪ Discussion Break-Outs	30 mins
▪ Report Outs	25 mins
▪ **Next Steps**	**5 mins**

Next Steps

Shared Learning:

- Key findings will be shared with the conference audience today

More Feedback to share?:

- Find us to speak during the meeting or reach out

What's coming?

- Incoming information continues to inform development of Draft 2

Thank You!

Please feel free to find us throughout the conference

DesignLights Consortium®

www.designlights.org