Pacific Northwest
NATIONAL LABORATORY

PNNL-34382

Cybersecurity Plan Review Summary

For Connected Communities

June 2023

Kris Willis
Paul Francik
Bora Akyol
Chance Younkin

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-34382

Cybersecurity Plan Review Summary

For Connected Communities

June 2023

Kris Willis
Paul Francik
Bora Akyol
Chance Younkin

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Contents

Tables

Acknowledgments

Cynthia Regnier, LBNL, Connected Communities National Coordinator lead

Acronyms and Abbreviations

CC	Connected Communities
CSP	Cybersecurity Plan
LBNL	Lawrence Berkeley National Laboratory
PNNL	Pacific Northwest National Laboratory

1.0 Introduction

As part of the Connected Communities (CC) Technical Assistance Program led by Lawrence Berkeley National Laboratory (LBNL), Pacific Northwest National Laboratory (PNNL) oversees the cybersecurity technical assistance for the CC cohort. PNNL's role is to provide a combination of provision of resources and technical assistance to support the development of successful cybersecurity plans for the Connected Communities cohort.

This Cybersecurity Plan (CSP) Review Summary provides an overview of activities to date in reviewing the 5 CSPs received so far:

Table 1. Members of the CC Cohort and dates of CSPs receipt and review

Project Name	CSP Received	CSP Reviewed
SunPower Corporation	1/30/2023	2/15/2023
IBACOS, Inc.	2/1/2023	2/15/2023
Spokane Edo		
Portland General Electric	9/28/2022	10/12/2022
Post Road Foundation		
Electric Power Research Institute		
Rocky Mountain Power / PacifiCorp	4/21/2023	4/24/2023
Slipstream		
OSU/MSI	3/9/2023	4/3/2023
Open Market ESCO		

The PNNL team awaits the 5 remaining CSPs and will review them upon receipt. Review times range from a few days to a few weeks from the time PNNL receives the CSP to the time feedback is provided to the cohort project. The time range is dependent on the complexity of the plan and availability of reviewers at the time of receipt.

PNNL is not involved in the scope and schedule of any of the CC projects and thus the PNNL team is not driving any deadlines for receipt of CSPs. Therefore, the PNNL review team simply awaits receipt of a CSP and makes every attempt to provide a review and feedback to the submitters in a timely fashion.

2.0 PNNL Approach

The PNNL CSP Review team has taken a proactive approach in reaching out to members of the cohort community. The team participates in the recurring CC Cohort calls, making announcements regularly about our availability and capability. PNNL also participates in these calls to learn the objectives, goals, and progress of the individual CC projects.

The PNNL team is also actively engaging with cohort members individually. PNNL has interacted with project leads and project cyber experts at various levels of detail to help the CC participants understand the value of the CSP, its purpose, the role of PNNL in CC, and how PNNL can help. This approach has solidified positive relationships between PNNL and the CC teams we have engaged, which will be very beneficial moving forward.

When it comes CSP reviews, PNNL has taken a passive role in soliciting members of the cohort to submit their plans. The intent here is to remain within our scoped task and to avoid enforcing schedules, thus building trust and relationship with cohort members. As these relationships with the cohort grow, PNNL will be in a trusted position to help with extremely important cybersecurity issues, reaching beyond mere reviews and feedback.

During interactions with CC project leads and cyber team members, either through phone calls or CSP reviews, the PNNL team encourages participants to deliver draft plans that represent their technical implementation describing in detail how they plan to secure their infrastructure. PNNL believes this approach will better prepare the cohort for any cybersecurity challenges faced throughout the project lifetime. This approach allows PNNL to better support and provide technical feedback beyond the review stage.

Our plan reviewers understand policy and standards for cybersecurity, building management, and grid security, but they are technical engineers seeking a detailed layout of the technical implementation, identification of their most critical assets, and a list of risks with potential mitigations. During the review process, the PNNL team makes recommendations based on experiences, and provides education to ensure plans are fundamentally secure by design.

3.0 Status of CSP Reviews

As Table 1 shows, PNNL has received 5 of 10 cybersecurity plans. Each plan received thus far has gone through an extensive review process where each plan was evaluated based on specific criteria within an evaluation checklist. The evaluation checklist is adapted from Appendix I of the Connected Communities FOA (DE-FOA-0002206) and is presented as Appendix A in this document. After each review the PNNL team sent the document back with feedback and recommendations and has then been available to project teams for discussion, assistance, and clarification. As of this writing, PNNL has not received any follow-on drafts for further feedback.

PNNL has observed that the submitted cybersecurity plans contain the right policy content but do not contain actionable implementation details. PNNL has discussed with LBNL, this lack of technical detail and the uncertainty of some received plans on their finalized team structure. Without teams having a solid foundation around their technical implementation, it's difficult for PNNL to recommend a plan to go forward past the review process. LBNL is aware of this issue and has increased PNNL's involvement within their scheduled cohort meetings to get a better sense of where teams are at.

From the reviews and engagements with the project teams so far, PNNL has concluded that many members of the cohort and the cyber experts working with them are concerned about implementing their CSP across their partnerships. They are also concerned about a potential lack of training for their partners. These concerns contribute to an additional concern that implementing cybersecurity and the expense of training could exhaust project budgets.

PNNL also observed that cyber-experienced organizations such as utilities may have challenges providing a cybersecurity plan that meets operational expectations in the complex nature of multi-party interactions regularly encountered in the CC projects.

As the remaining CSPs are delivered to PNNL for review, the team will continue to provide recommendations and feedback to address these issues.

4.0 Next Steps

In addition to performing reviews for the remaining CC projects, PNNL will implement a Phase 2 for cybersecurity technical assistance. Phase 2 will address the concerns described in Section 3.0 and solidify active, ongoing engagements with the PNNL Cybersecurity Technical Assistance team, the CC cohort project members, and the National Coordinator team at LBNL. In Phase 2, the PNNL team will implement these new cyber-focused mechanisms:

Office hours. Office hours will help teams build their cybersecurity plan, identify security gaps, and help cohort members solidify their technical implementation. Each office hour session will be structured to provide education and assistance on prioritized topics. After each structured topic, participants will have the opportunity to ask unique questions about their project and to receive one-on-one assistance.

Working group. The working group will be a forum where the PNNL team will be consistently available one hour of each week. Members of the CC cohort can dial in with any questions, issues, concerns they have. The office hours will include a monthly seminar series featuring presentations on cybersecurity from cohort members, PNNL personnel, and invited speakers from the industry.

Mailing list. The mailing list will be used to disseminate timely and relevant information, schedule seminars, and to increase communication among cohort members. This will differ from the National Coordinator's CC Cohort Leads mailing list in that it will contain contacts specifically working on and interested in cybersecurity activities.

Small-scale sample CSP. PNNL will develop simple, exemplary cybersecurity plan to provide to the cohort. This will give the cohort a better idea what should be presented within their unique project's cybersecurity plan.

PNNL has requested additional funding from DOE to provide extended capabilities in the form of scenarios, comprehensive example CSPs, and training for the CC Cohort and beyond. If this request is granted, PNNL will embark on activities such as:

- A modernized cybersecurity plan checklist to replace Appendix I of the FOA
- A comprehensive template for cybersecurity plans that can be used by the CC cohort and across the DOE complex
- A scenario-based set of examples and training materials that DOE can provide to CC, and across the DOE complex

5.0 Conclusion

To conclude, PNNL has had successful engagement with most members of the CC Cohort, reviewed 5 CSPs with 5 more projects yet to submit. The effort to date has yield a much better understanding by PNNL of the CC cybersecurity needs and led to an updated plan of attack for the remainder of this FY and into FY24.

With the Phase 2 implementation, PNNL expects to increase engagement and influence, leading to further reviews of all 10 project CSP going forward. The CC cohort recognizes the importance of cybersecurity and has come to rely on PNNL for not only CSP reviews, but also as an organization that can provide recommendations, assistance, and a mechanism to promote consistency and sharing of ideas among the cohort.

Overall, PNNL team believes the review process, the engagements with the cohort, and the leadership of LBLN as the National Coordinator has been extremely successful and can improve throughout this FY and into the future.

Appendix A – CSP Checklist for cohort projects

Does your Cybersecurity Plan…

Cover and remain active for the full lifecycle of the proposed solution, including:

- ☐ Design
- ☐ Implementation
- ☐ Maintenance
- ☐ Disposition

Use standards and best practices to a reasonable degree

- ☐ Criteria for selecting standards and best practices
- ☐ Use or adoption of cybersecurity best practices and standards
- ☐ Use or adoption of emerging smart grid standards
- ☐ Methods for achieving compliance with selected standards
- ☐ Deviations from selected standards
- ☐ Proposed alternatives to selected standards when they are missing or inadequate

Define an approach for

- ☐ Ensuring confidentiality, integrity, availability
- ☐ Secure logging, monitoring, alarming, and notification
- ☐ Executing “defense in depth”
- ☐ The use of open standards to the extent possible
- ☐ Community resources when practical

Focus properly on the environment of the proposed solution, specifically:

- ☐ Within the system/network of the proposed solution
- ☐ On the boundaries and the external interfaces of the proposed solution
- ☐ On all other interfaces of the proposed solution

Identify and address unacceptable consequences that could occur from:

- ☐ Insider threat
- ☐ External adversaries
- ☐ User errors
- ☐ Natural disasters

Identify and address threats such as:

- ☐ Spoofing
- ☐ Tampering
- ☐ Repudiation
- ☐ Information Disclosure
- ☐ Denial of Service
- ☐ Elevation of Privilege

Identify and address vulnerabilities through:

- ☐ Structural Security
- ☐ Operational Security

Summarize the risks and mitigations for the full lifecycle of the proposed solution, including:

- ☐ Design
- ☐ Implementation
- ☐ Maintenance
- ☐ Disposition

Discuss cybersecurity criteria for:

- ☐ Selecting vendors
- ☐ Selecting devices

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov