IBR Digital Supply Chain Gap Analysis and Recommendations

Ryan Cryar, Cybersecurity Researcher

S2G Solar Supply Chain Workshop

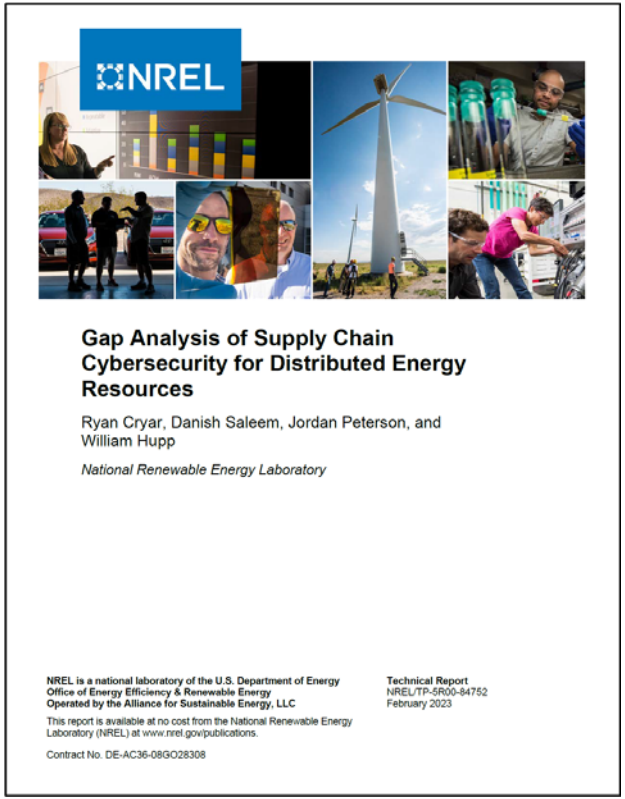
August 1st, 2024

Introduction

- Presidential Executive Order 14017 for supply chain cybersecurity
- The Securing Solar for the Grid (S2G) project supported research for supply chain cybersecurity through:
  - Performing gap analysis of current cybersecurity landscape of distributed energy resources (DER)
  - Creating recommendations for the digital supply chain cybersecurity of solar photovoltaics
  - Engaging with academia, national laboratories, and industry to address and understand digital supply chain challenges

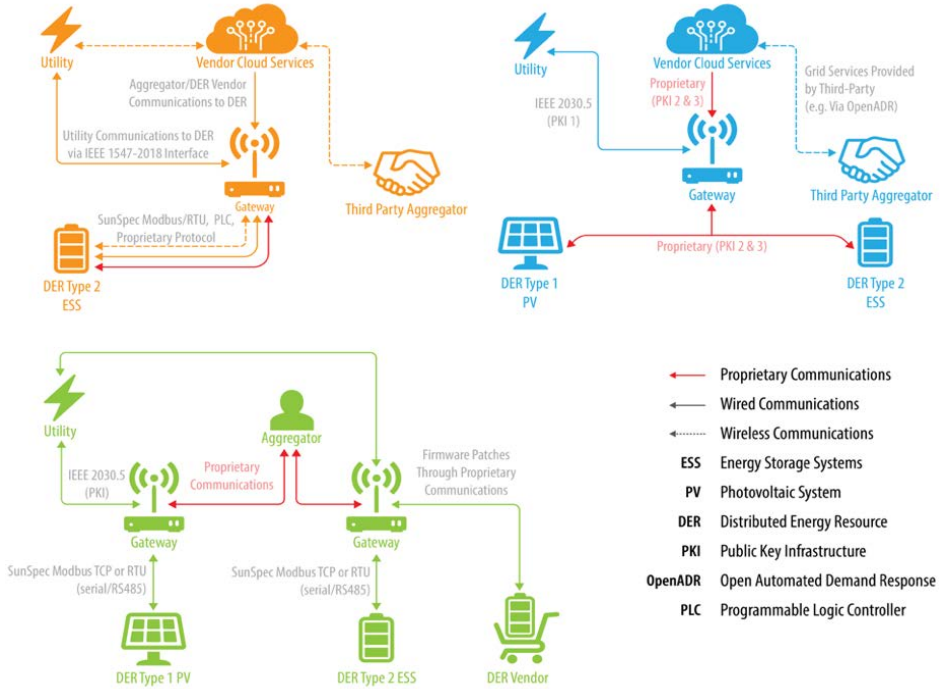
Gap Analysis

- *Gap Analysis of Supply Chain Cybersecurity:*
  - Addresses the landscape of the digital supply chain
  - Drafts the ideal state of the digital supply chain
  - Provides recommendations to bridge gaps between the current and ideal
- Primary gaps stem from challenges related to open-source software, standards, and where to apply best practices.



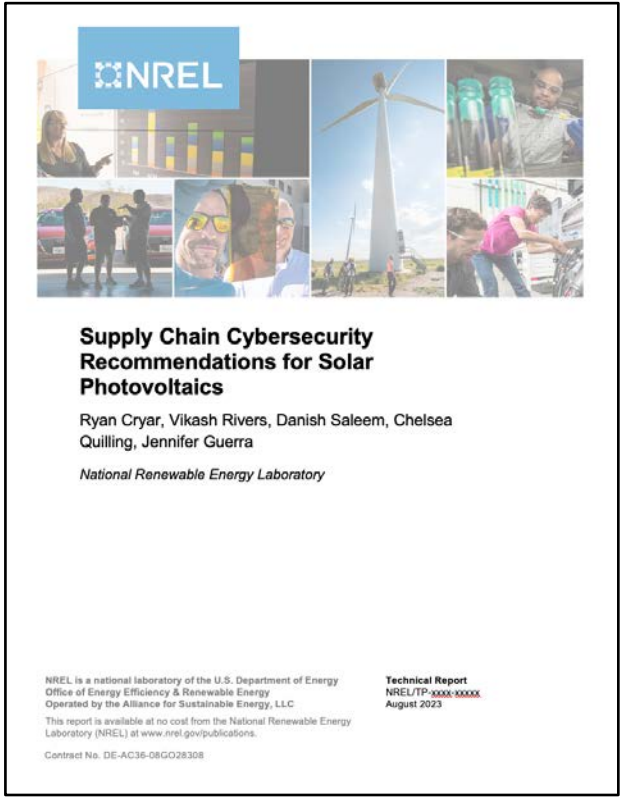
Gap Analysis cont.

- Software guidance:
  - Where to apply best practices
  - Continuous monitoring
  - Open source
- Legacy hardware:
  - Secure updates and lack of update support
- Standards and recommendations:
  - Interoperability
  - Role and responsibility delineation
- Distributed supply chains:
  - Heterogenous
  - Connected devices
- Who owns what part of the risks?



Synthesizing Recommendations

- *Supply Chain Cybersecurity Recommendations for Solar Photovoltaics:*
  - Follows prior work
  - Addresses practices found and adapted from NERC, NIST, and NATF
  - Provides down-selected recommendations that could apply to supply chain cybersecurity for solar photovoltaics
  - Focuses on short, clear language that can be testable and quantified
- Publication released on NREL's website.



Synthesizing Recommendations cont.

The report includes:

- Recommendations that range from governance to implementation
- Language on which stakeholders the recommendation apply to
- Acquisition practices informing ownership and supply chain traceability
- Guidance on managing risk throughout the supply chain lifecycle

Table of Contents

Example Recommendations

- **Recommendation 30**: Through a secure portal, vendors should provide customers with a vulnerability disclosure report, including the analysis and findings describing the impact that a reported vulnerability has on a product as well as plans to address the vulnerabilities. The vulnerability disclosure report should be signed with a trusted, verifiable, private key that includes a time stamp of the signature. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire RISK-08)

- **Recommendation 31**: Vendors should establish a separate notification channel for customers in case a vulnerability arises that is not included in the vulnerability disclosure report. (Adapted from NIST SP 800-161r1 RA-5; NATF Energy Sector Supply Chain Risk Questionnaire VULN-06, VULN-07)

Concluding thoughts

- Strengthening supply chain cybersecurity is a large undertaking and an ever-evolving problem
- Continuously monitor and assess downstream suppliers and your own practices
- Leverage industry engagement through working groups to continue the conversation and improve visibility into challenges

Photo by Dennis Schroeder, NREL 22168

Thank You!

Let’s work together!

Ryan.Cryar@nrel.gov

NREL/PR-5T00-90873

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

NREL
Transforming ENERGY