

Funded by:



**SOLAR ENERGY  
TECHNOLOGIES OFFICE**  
U.S. Department Of Energy



# DER Digital Supply Chain Gap Analysis

Ryan Cryar, Cybersecurity Researcher  
Securing Solar for the Grid Workshop  
September 14<sup>th</sup>, 2023

---

Principal Investigator: Danish Saleem

Other Contributors: Ryan Cryar, Jennifer Guerra, Chelsea Quilling

- Presidential Executive Order 14017 for supply chain cybersecurity
- This project supported research for supply chain cybersecurity by:
  - Performing gap analysis of current cybersecurity landscape of distributed energy resources (DERs)
  - 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.
- Identified future opportunities to engage with industry members through different cybersecurity working groups.



- *Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources:*
  - 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.
- Challenges stem from areas such as open source, standards, and where to apply best practices.



## Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

*National Renewable Energy Laboratory*

NREL is a national laboratory of the U.S. Department of Energy  
Office of Energy Efficiency & Renewable Energy  
Operated by the Alliance for Sustainable Energy, LLC  
This report is available at no cost from the National Renewable Energy  
Laboratory (NREL) at [www.nrel.gov/publications](http://www.nrel.gov/publications).

Technical Report  
NREL/TP-5800-84752  
February 2023

Contract No. DE-AC36-08G028308

# Addressing Recommendations

Funded by:



- 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 that could apply to the digital supply chain of solar photovoltaics
  - Focuses on short, clear language that can be testable and quantified
  - Includes recommendations reviewed by academia and national laboratories
- Publication released on NREL website



## Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Ryan Cryar, Vikash Rivers, Danish Saleem, Chelsea Quilling, Jennifer Guerra

*National Renewable Energy Laboratory*

NREL is a national laboratory of the U.S. Department of Energy  
Office of Energy Efficiency & Renewable Energy  
Operated by the Alliance for Sustainable Energy, LLC  
This report is available at no cost from the National Renewable Energy  
Laboratory (NREL) at [www.nrel.gov/publications](http://www.nrel.gov/publications).

Contract No. DE-AC36-08GO28308

**Technical Report**  
NREL/TP-xxxx-xxxxx  
August 2023

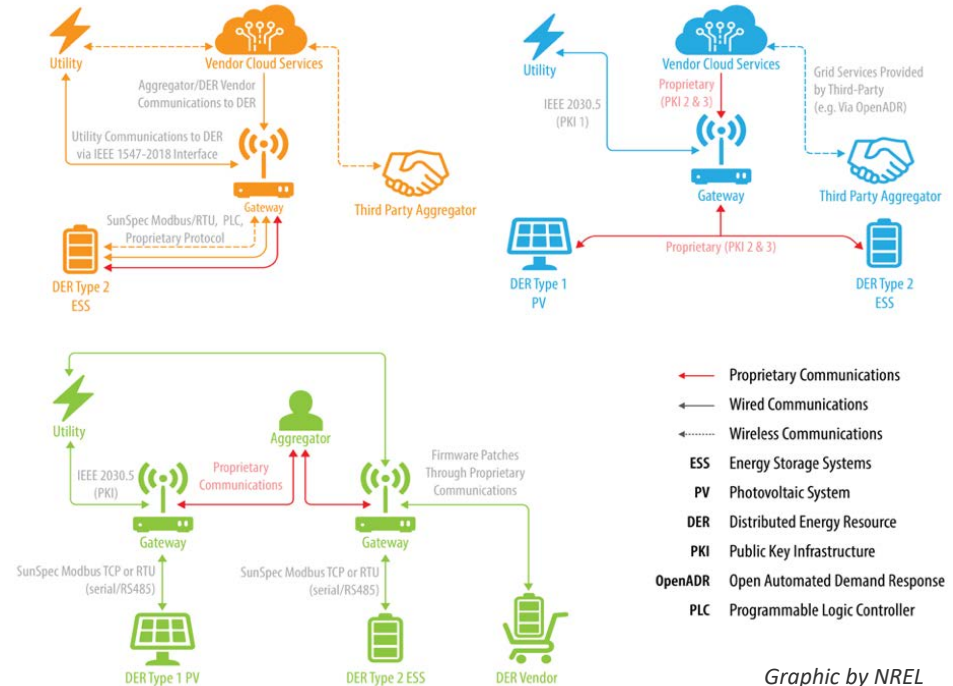
# Example Recommendations

---

- **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)


# Outcomes of the Reports

- Interest in forming a subgroup on supply chain cybersecurity within SunSpec/Sandia Cybersecurity Working Group
- Engage with industry members to develop more effective recommendations.
- Provide immediate value to industry through recommendations that are testable.
- Gaining visibility into the challenges of the digital supply chain of renewable energy resources.








# Future Work

- By leveraging the SunSpec/Sandia cybersecurity working group to create a subgroup on supply chain cybersecurity, further adapt the recommendations.
- Through this subgroup, to the extent possible, harmonize with other groups, such as SEPA CSWG, CPUC Smart Inverter Working Group, and UL 2941 Technical Committee.
- With this engagement, industry members see immediate value by actively developing recommendations that can be tailored to their own practices.



### SunSpec/Sandia DER Cybersecurity Workgroup



<p><b>DER Cybersecurity Certification Procedure</b></p> <ul style="list-style-type: none"><li>• Defined standardized procedure for DER vulnerability assessments.</li><li>• Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)</li><li>• Publication: "Certification Procedures for Data and Communications Security of Distributed Energy Resources"</li><li>• Future work: Expected development within UL 2900-2-4 STP</li></ul> 	<b>Complete</b>	<p><b>Secure Network Architecture</b></p> <ul style="list-style-type: none"><li>• Created DER reference architecture best practice.</li><li>• Lead: Candace Suh-Lee (EPRI)</li><li>• Publication: "EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design"</li><li>• Future work: Risk-based approach adopted in IEEE 1547.3</li></ul> 	<b>Complete</b>
<p><b>Data-in-Flight Requirements</b></p> <ul style="list-style-type: none"><li>• Encryption, authentication, and key management requirements.</li><li>• Lead: Ifeoma Onunkwo (Sandia)</li><li>• Publication: "Recommendations for Trust and Encryption in DER Interoperability Standards", another covering Data-in-Transit Requirements document (forthcoming).</li><li>• Future work: IEEE 1547.3 update, IEEE 2030.5 revisions.</li></ul> 	<b>Complete</b>	<p><b>Access Control</b></p> <ul style="list-style-type: none"><li>• DER Role-Based Access Control recommendations.</li><li>• Lead: Jay Johnson (Sandia)</li><li>• Topics: Access control taxonomy and security models</li><li>• Planned Publication: "Recommendations for Distributed Energy Resource Access Controls"</li><li>• Future work: Add recommendations to IEEE 1547.3 Guide</li></ul> 	<b>Wrapping Up</b>
<p><b>Patching Requirements</b></p> <ul style="list-style-type: none"><li>• Establishing patching guidelines for DER devices and DER networking equipment.</li><li>• Starting August-Sept 2020. Lead: TBD</li><li>• Topics: Patching update rates, maintenance guidelines, etc.</li></ul>	<b>Starting!</b>	<p><b>Utility/Aggregator Auditing Procedure</b></p> <ul style="list-style-type: none"><li>• Creating recommended auditing practices for DER networks.</li><li>• Planned for March-April 2021. Lead: TBD</li><li>• Topics: Step-by-step auditing procedure for internal or external compliance review. Recommend data for attack forensics.</li></ul>	<b>Q2 FY21</b>

# Industry Engagement

Funded by:



- Engagement with industry is prioritized.
- Several working groups are being leveraged to provide balanced feedback among multiple types of stakeholders and participants.
- Additional engagement sources are actively being sought.



*Photo by Dennis Schroeder, NREL 22168*



# Thank You!

---

Let's work together!

[Ryan.Cryar@nrel.gov](mailto:Ryan.Cryar@nrel.gov)

NREL/PR-5R00-87282

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.