INL/CON-24-78523-Revision-0

Developing a Supply Chain Security Program

June 2024

Megan Jordan Culler, John Clay Bell II, Emma Mary Stewart, Remy Vanece Stolworthy

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-78523-Revision-0

Developing a Supply Chain Security Program

Megan Jordan Culler, John Clay Bell II, Emma Mary Stewart, Remy Vanece Stolworthy

June 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

PROJECT NAME: Developing a Supply Chain Security Program

Project Lead(s): **Megan Culler**
Lead Organization(s):**Idaho National Laboratory**
PI Email: **megan.culler@inl.gov**

BACKGROUND and OVERVIEW

- Growing concerns over dominance of foreign supply chain for critical energy infrastructure
  - Availability, quality control, number of parties with influence, etc.
- Cyber considerations for key digital components
- Lab approach at the micro-to-macro scale
  - Evaluation of devices
  - Technical assistance to owners & operators
  - Landscape analysis to understand national exposure

COMPONENTS / METHODS

- *Industry supply chain analysis:*
  - What are the key digital components?
  - Where are the suppliers located?
  - Where are the parts actually manufactured?
- *Component criticality breakdown*
  - Connectivity (attack exposure)
  - Impact (consequence of failure)
- *Vulnerability analysis* – several tools and projects
- *CIE approach to mitigating risk*

KEY SUCESSES / MILESTONES

- Coordination across labs for solar supply chain analysis: SBOM, HBOM, vulnerability analysis
- Quick mobilization to support asset owners in understanding risk of existing and future BESS installations.
- HBOM Catalog and vulnerability tracking developed for wind controllers and other devices

TAKE-AWAYS

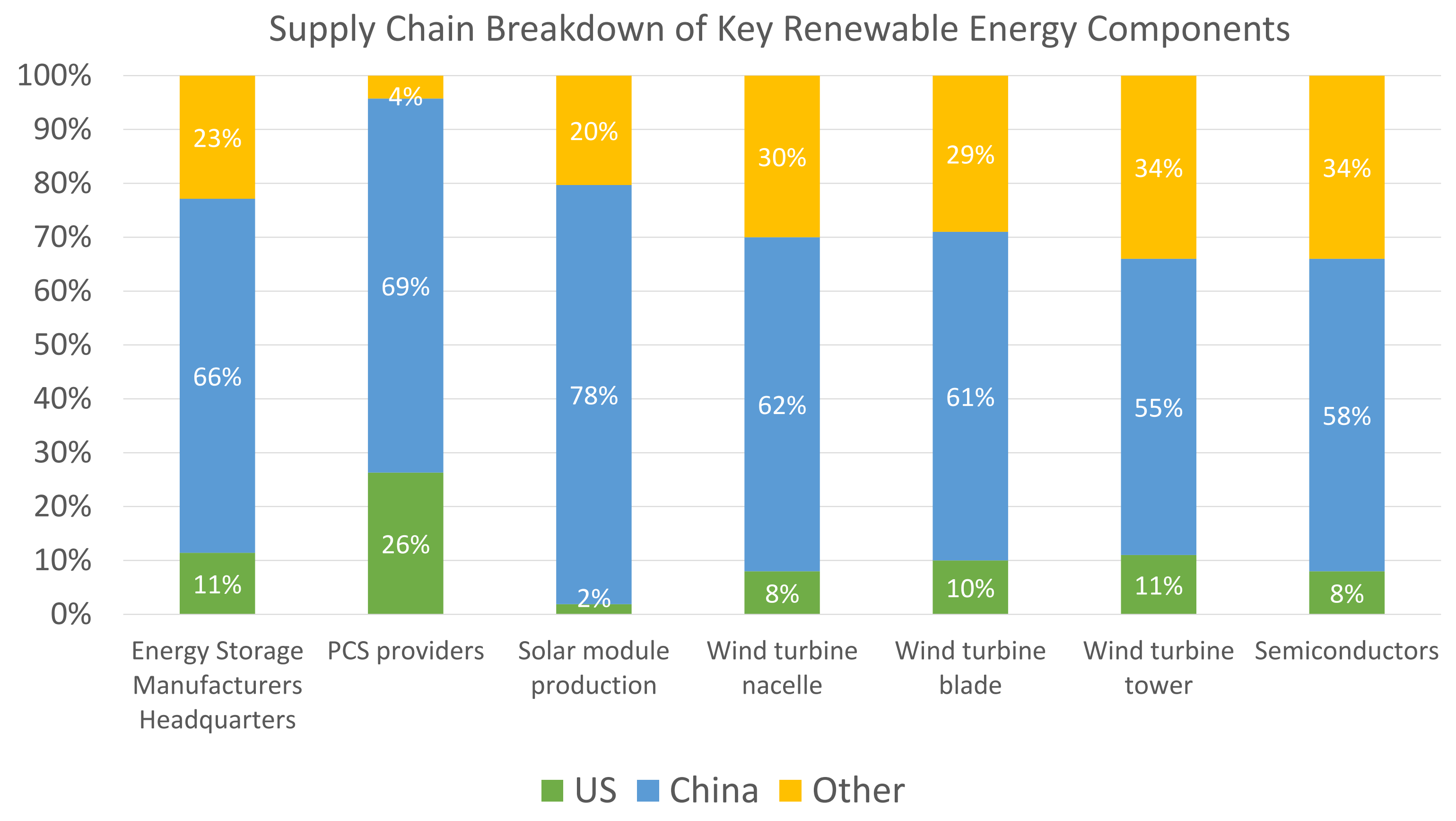
- Supply chain risks exist across the grid, and supply chain security risks continue to grow with increased digitization.
- A good asset inventory is necessary before other supply chain security concepts can be effectively implemented.
- Patches should be applied as quickly as possible, still following good testing and approval practices to ensure there is no disruption to operational environments.
- DOE research is examining ways to support asset owners and evaluate the risk from a national level.

INL/CON-24-78523

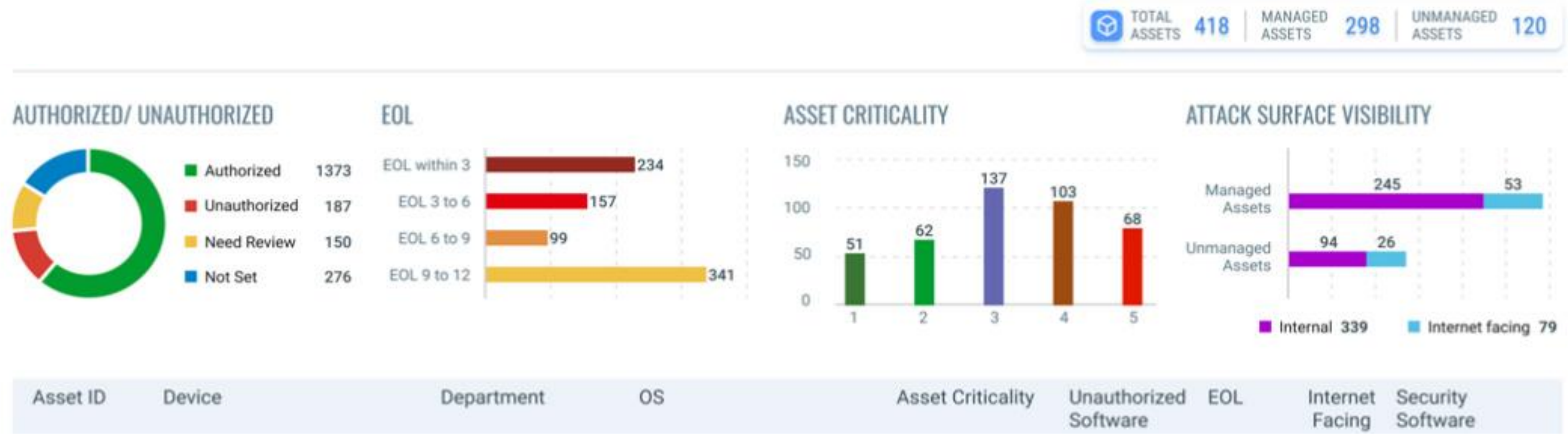
Amid growing concerns over foreign manufactured equipment deployed in critical energy infrastructure, a supply chain security program goes a long way towards mitigating risk.

Co-op Cyber Tech

NRECA America's Electric Cooperatives

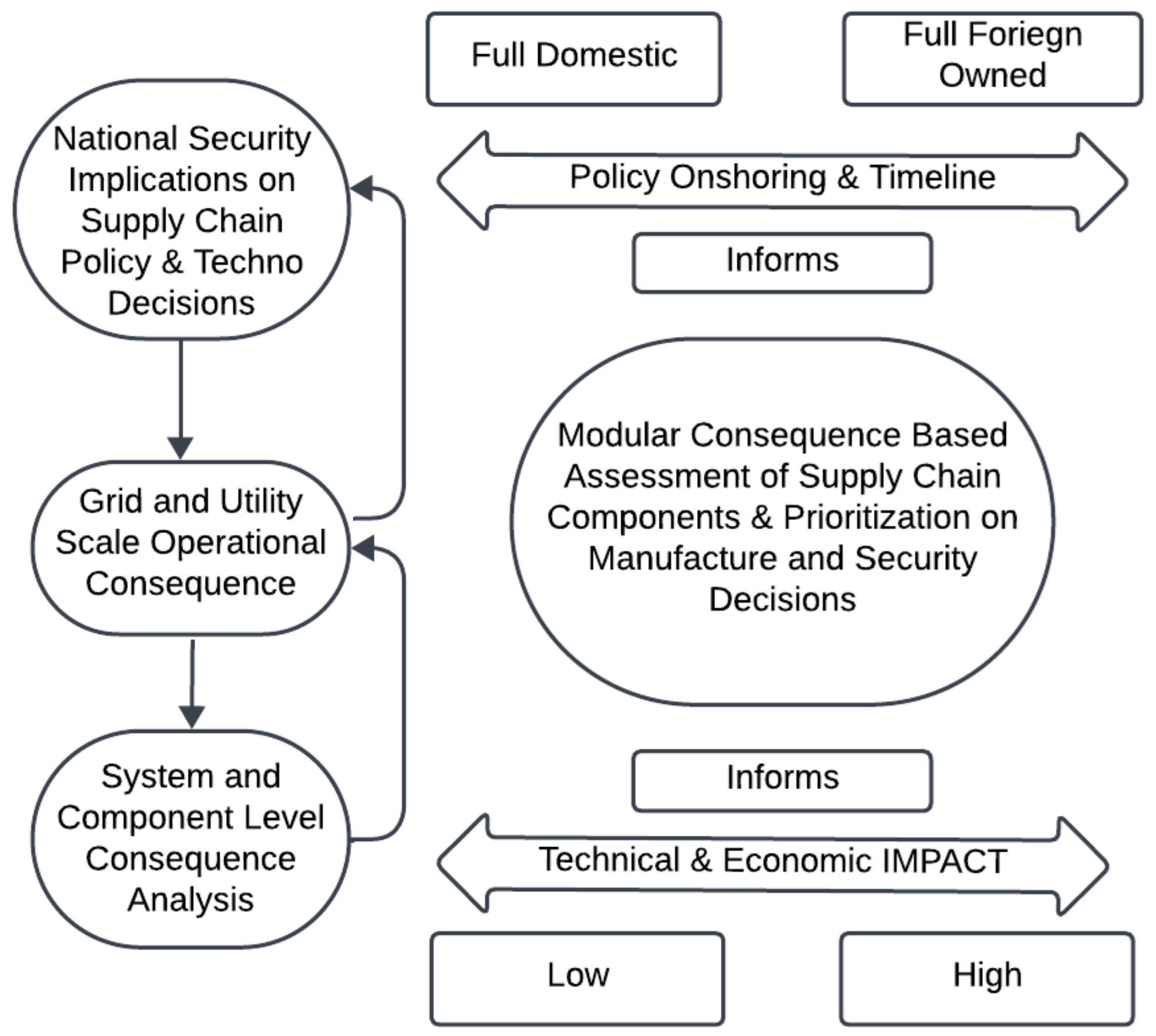

Supply Chain Breakdown of Key Renewable Energy Components

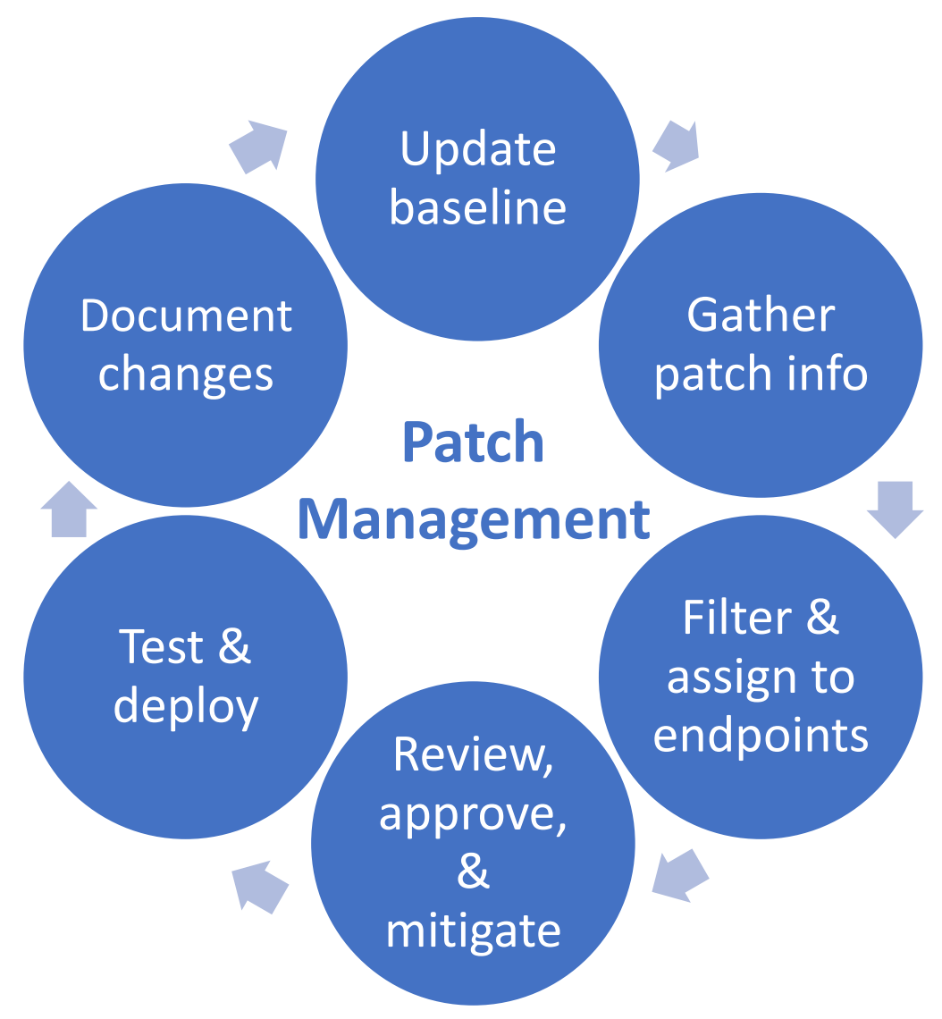
Critical components for modern energy systems are highly dependent on foreign companies and manufacturing, no matter how it is broken down. The transition to a digitized grid underscores the need for a robust, resilient, and secure supply chain.



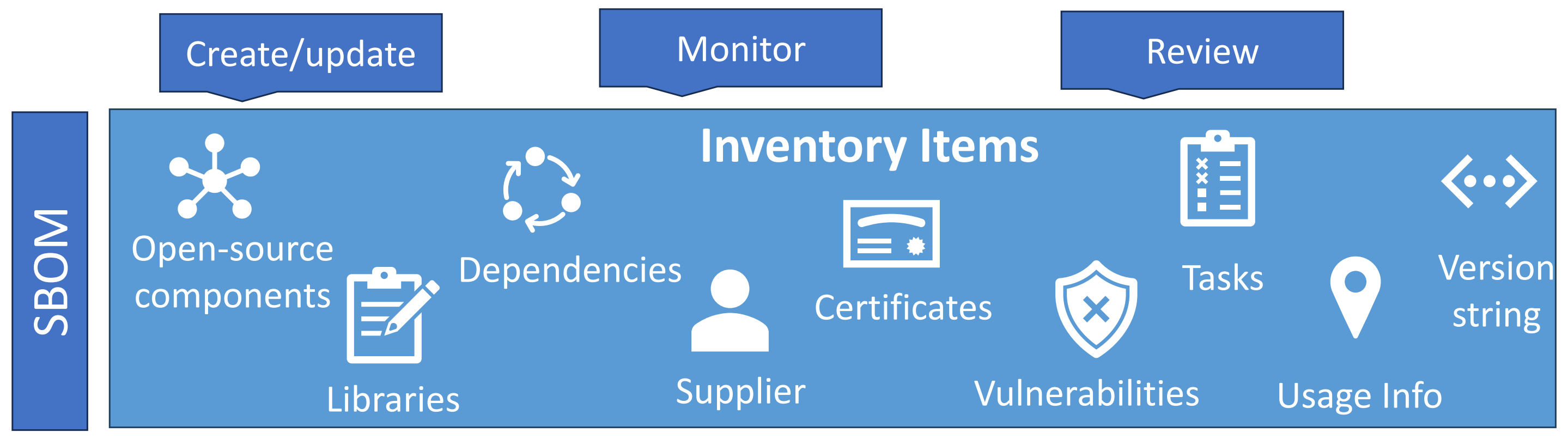
Asset Inventory is critical to supply chain security. Building a baseline of components and actively maintaining it to accurately reflect what is in the field gives asset owners and operators the awareness to perform more in-depth risk assessment. As noted in the mock dashboard above, asset inventories may track exposure of devices based on network placement, asset criticality, asset support from vendors, asset management (managed/unmanaged) and more.

Research is addressing supply chain security on many fronts. This framework cascades from a macro to a micro perspective, focused on a risk-based approach that considers the source and foreign influence over components, the impact of individual components and potential for consequential events. Results from this analysis will identify repeatable methodologies for assessing supply chain cyber risk for electric energy organizations.


Full Domestic
Full Foriegn Owned
National Security Implications on Supply Chain Policy & Techno Decisions
Policy Onshoring & Timeline
Informs
Grid and Utility Scale Operational Consequence
Modular Consequence Based Assessment of Supply Chain Components & Prioritization on Manufacture and Security Decisions
System and Component Level Consequence Analysis
Informs
Technical & Economic IMPACT
Low
High



Patch Management is the process of tracking and applying fixes for software bugs or security flaws released by vendors. Patches can only be applied if the user is tracking the equipment and software in their systems. Patches should be applied quickly, as events have demonstrated that adversaries quickly exploit disclosed vulnerabilities, but this can be difficult in operational environments.



Software bill-of-materials (SBOMs) provide detailed information about the software components of key digital infrastructure. SBOMs are built to be machine-readable and can help automate vulnerability awareness.

Additional project contributors: John C. Bell, Emma Stewart, Remy Stolworthy,