Overview of the BESS Procurement Guide

The battery energy storage system (BESS) Procurement Guide provides industry-informed best practices for BESS supply chain security. This guide, intended for BESS Consumers, fits within an entity-specific supply chain risk management (SCRM) program.

This BESS Procurement Guide helps integrate digital energy infrastructure quickly by developing and maturing cybersecurity supply chain risk management programs. This will help BESS Consumers manage non-domestic equipment appropriately.

SUPPLY CHAIN SECURITY FOR BESS AND IBR

BESS, inverter-based resources (IBR), and other energy sector digital equipment could present security risks due to the nature of their setup. Considerations include persistent communications, organizational challenges with foreign ownership, and unknown spiderwebs of components. Many of these challenges can be aided with enhanced SCRM focused on procurement processes and contract terms.

Through procurement guidance that integrates SCRM considerations, organizations can mitigate supply chain risks from the start. Some of the guidance focuses on eliminating risk, while other guidance introduces risk transferal. This requires other stakeholders to take on some of the responsibilities of ensuring security of components throughout their lifecycles.

Some key cybersecurity challenges present in the majority of digital equipment include:

- Remote monitoring and control capabilities, expanding adversary attack surface.
- Remote software and firmware update capabilities. This allows suppliers to quickly deploy patches, but also exposes the equipment to the potential of malicious firmware uploads.
- Reliance of critical systems on the software and firmware in digital equipment.
- Capability to rapidly change the functionality or behavior of devices through malicious or error-filled code updates.
- Proliferation of stakeholders who need, or claim to need, access to digital devices and their data.
- Supply chain security risks introduced in multiple points of the production process: design, procurement of sub-components

Idaho National Laboratory

(e.g. processing chips), manufacturing, assembly, shipping, etc.

Some enhanced risks present in equipment from Foreign Entity of Concern (FEOC) organizations:

- Less regulation or oversight of design and manufacturing process, which may allow lower quality manufacturing or design to slip though.
- Potential for foreign governments to require FEOCs to take adversarial action in accordance with their own laws.
- Potential for foreign governments to require FEOCs to provide customer information and/or proprietary information about equipment which could be used to plan adversarial action against the end users.

INTEGRATING CYBERSECURITY REQUIREMENTS INTO PROCUREMENT PROGRAMS

The procurement function plays a critical role in the effective management of BESS, IBR, and other energy sector digital system supply chain cybersecurity risks. By implementing cybersecurity considerations as part of the vendor selection and purchase processes, the organization sets a standard for vendor security maturity.

There are a few important steps to drive secure supply chain objectives. Development of key controls standards should happen as part of the bidding and selection processes for any vendors associated with critical digital components. Intake analysis guidelines should be used to determine what type of risk assessment is required. A formal risk assessment methodology for selected vendors of products and services should be defined.

While a comprehensive SCRM program is recommended, given the criticality of implementing immediate near-term controls, three critical foundational elements are presented for procurement processes that will mitigate many of the highest consequence cyber supply chain risks:

- **BESS Request for Proposal (RFP) & Solicitation Requirements** – This section includes bid process requirement recommendations to improve bid processes and reduce lags in timeline once security requirements are integrated. It also includes guidance on initial and outreach communications to establish applicable cyber and supply chain security requirements. As part of the initial setup, any procurement initiative to manage vendors requires a compressive inventory of all suppliers. The guide provides a risk-based approach to developing a supplier inventory.
- **BESS Vendor Risk Assessment** – This section contains a basic risk analysis and impact factors, decision trees for initial evaluation, and risk assessment methodology guidelines. It includes context for the BESS vendor assessment in the context of organizational risk. It discusses cyber supply chain security risk considerations specific to BESS, IBR, and energy digital equipment. The methodology provides guidance for classifying service and product suppliers into three tiers corresponding to low, medium and high risk.
- **BESS Procurement Agreement Terms** – This section provides sample terms and conditions for vendor agreements to mitigate security and supply chain risks associated with procurement of digital assets and services. The guidance includes software and hardware bill of materials requirements. The sample terms cover topics including disclosure of security events, incident response, vulnerability disclosure, access to systems, and more. Supplier management controls to ensure cyber SCRM processes are effectively integrated by both suppliers and the organization.

For additional information on INL Digital Assurance project initiatives and other available resources visit www.inl.gov/national-security/csdet/.

FOR MORE INFORMATION

Technical contact
Emma Stewart
emma.stewart@inl.gov

General contact
Tracy Briggs
tracy.briggs@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory