



Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance

October 2024

Changing the World's Energy Future

Emma Mary Stewart, Remy Vanece Stolworthy, Shari Gribbin, Tracy Lee Briggs, Megan Jordan Culler



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.

Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance

**Emma Mary Stewart, Remy Vanece Stolworthy, Shari Gribbin, Tracy Lee Briggs,
Megan Jordan Culler**

October 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**



Securing Digital Energy Infrastructure

Procurement, Contracting and Supply
Chain Risk Management Guidance



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.

Battery Supply Chain Security: Procurement Guidance and Sample Contract Terms

**Emma Stewart, Megan Culler, and Remy Stolworthy
Idaho National Laboratory
Shari Gribbin
CNK Solutions**

October 2024

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

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

Page intentionally left blank

CONTENTS

ACRONYMS	viii
1. INTRODUCTION.....	1
1.1. Intended Audience	1
1.2. Purpose.....	2
1.3. Trends in Supply-Chain Cybersecurity Policy.....	3
1.4. Introduction to Battery Energy Storage Systems and Inverter-Based Resources Supply-Chain Security	5
2. MATURING BESS SUPPLY-CHAIN CYBERSECURITY: GENERAL OVERVIEW	6
2.1. Introduction to Cybersecurity SCRM Programs	6
2.2. Integrating Cybersecurity Requirements into Procurement Programs.....	8
3. MATURING BESS CYBER SUPPLY CHAIN SECURITY: PROCUREMENT BIDDING AND SELECTION PROCESSES	9
3.1. Vendor Selection Processes	9
3.2. Vendor Inventory and Management Controls.....	9
4. MATURING BESS SUPPLY-CHAIN CYBERSECURITY: VENDOR RISK ASSESSMENT	10
4.1. Organizational Risk Overview	10
4.2. Defining Organizational Cybersecurity-Risk Assessment Priorities for BESS, IBR, Energy Digital-Equipment Products and Services	10
4.3. BESS Supply-Chain Cybersecurity Risk Considerations	11
4.4. BESS Vendor Intake: Initial Screening, Analysis, Risk Assessment and Exception Processes	13
4.4.1. Sample Decision Tree for Initial Analysis of Service Suppliers.....	14
4.4.2. Sample Decision Tree for Initial Analysis of Products, Assets, and Equipment Suppliers	14
4.4.3. Out-of-Process Procurements and Exceptions	15
4.5. BESS Vendor Cybersecurity Risk-Assessment Methodology.....	16
4.5.1. General Considerations for Assessment Methodology/Process.....	17
4.5.2. Completing the Vendor Evaluation.....	18
4.5.3. Final Approvals, Selection Confirmation, Formal Agreement, and Vendor Communications	22
5. MATURING BESS CYBER SUPPLY CHAIN SECURITY: VENDOR AGREEMENTS AND PROCUREMENT TERMS	23
5.1. Procurement Agreements	23
5.2. Sample Procurement Agreement Terms	24
5.3. General Terms.....	24

5.4.	General Product and Services Cyber and Supply Chain Security	24
5.5.	Enterprise Cybersecurity and Supplier Cyber Hygiene Requirements	29
5.6.	BESS Product- and Service-Related Security Terms.....	31
6.	MATURING BESS SUPPLY-CHAIN CYBERSECURITY: SUPPLIER MANAGEMENT AND COMPLIANCE CONTROLS	32
7.	CONCLUSION	32
8.	REFERENCES.....	33
	Appendix A Sample Procurement Agreement:.....	34
	Contract Definitions.....	34

FIGURES

Figure 1:	Intended audience for the BESS Procurement Guide.....	2
Figure 2:	The Purdue model represents BESS, highlighting the connectivity and digitization of energy assets increasingly relied upon for grid stability and reliability.	4
Figure 3:	DOE supply-chain cybersecurity principles. [5]	5
Figure 4:	BESS components and potential suppliers.	5
Figure 5:	Framework for SCRM program architecture with examples of implementing controls.	7
Figure 6:	This BESS Procurement Guide focuses on prioritized SCRM program elements: procurement and vendor requirements, risk assessment; and vendor agreements.....	7
Figure 7:	Basic cybersecurity guidance for a SCRM procurement program.	8
Figure 8:	Sample initial-analysis risk decision tree for service suppliers.	14
Figure 9:	Sample decision tree for initial analysis of products, assets, equipment, or suppliers.	15
Figure 10:	BESS vendor cybersecurity risk-assessment methodology summary.....	16
Figure 11:	Three major steps to complete a supplier evaluation.	18
Figure 12:	Legal Disclaimer, BESS procurement guide Sample Procurement Agreement Terms.....	24

Page intentionally left blank

ACRONYMS

AC	Alternating current
BABA	Build America Buy America Act
BESS	Battery Energy Storage Systems
BMS	Battery Management System
CAISO	California Independent System Operator
CATL	Contemporary Amperex Technology Co. Limited
CCE	Consequence-driven Cyber-Informed Engineering
CIE	Cyber-Informed Engineering
DC	Direct current
DER	Distributed Energy Resource
DOE	Department of Energy
EBOS	Electrical Balance of System
ENISA	European Network and Information Security Agency
ESP	Encapsulating-Security-Payload
EV	Electric vehicle
FAQ	Frequently Asked Questions
FERC	Federal Energy Regulatory Commission
FEOC	Foreign Entity of Concern
FMEA	Failure Mode and Effects Analysis
IBR	Inverter-based resource
ICS	Industrial control system
IE	Interdependency Evaluation
INL	Idaho National Laboratory
IP	Internet Protocol
MSOC	Minimum State-of-Charge
MW	Megawatt
NDAA	National Defense Authorization Act
NERC	North American Electric Reliability Corporation
OT	Operational technology
PCS	Power conversion system
QA	Quality assurance
RFP	Request for proposal
SCADA	Supervisory control and data acquisition
SCRM	Supply Chain Risk Management
TA	Technical Assistance
U.S.	United States

Page intentionally left blank

Battery Supply Chain Security: Procurement Guidance and Sample Procurement terms

1. INTRODUCTION

The energy sector stands at a crossroads, facing the dual imperative of accelerating the transition to sustainable energy systems while simultaneously securing a supply chain that is both robust and resilient. Batteries and associated power electronic interfaces are key components to clean energy and more-resilient energy delivery. This transition also requires the prioritization of reliability, safety, and security within the asset infrastructure and its use within the energy-delivery systems more broadly.

While there is significant benefit to modernization and digitization of U.S. infrastructure through the Bipartisan Infrastructure Law and other federal programs, our renewable- and clean-energy supply chains (in particular, for battery energy-storage systems (BESS) and associated digital control equipment) have limited capacity to source necessary digital assets through U.S. or allied sources [1]. This challenge underscores the need to secure the components and technology being procured and configure the contract and technology in such a way the components can be operated with confidence for years to come. Substantial investments in semiconductors and other manufacturing capabilities will impact U.S. supply chains. While those supply chains mature, however, U.S. asset owners will need to continue leveraging other available equipment sources to meet their goals and maintain costs. In that interim period, they must also focus on developing and implementing robust supply-chain risk-mitigation programs to counter the risks posed by foreign-sourced supply chains and globally immature security practices. Failure to mitigate these risks could negatively impact the overall transition and more directly impact grid reliability and safety in the power systems these BESS support.

Recognizing the scale of this industry challenge, the United States (U.S.) Department of Energy (DOE) Grid Deployment Office (GDO) and Office of Cybersecurity Energy Security and Emergency Response have launched a multi-year BESS supply-chain security initiative to identify consequence-driven approaches to addressing BESS supply-chain security and provide resources to support prioritization of security efforts associated with the supply chain of BESS equipment and services. This guide is one element supporting these resources. It sets forth a framework and guidance for procurement bidding, selection, risk analysis, and agreement terms stakeholders can implement to mitigate cybersecurity risks across the entirety of battery-system component ecosystem, including the interconnected software and hardware required for control and monitoring BESSs.

1.1. Intended Audience

This guide was developed for entities procuring BESS equipment and may also apply to entities procuring inverter-based resources (IBRs), distributed-energy resources and other digital energy systems and services with slight modifications. This population includes storage-asset owners, utilities, government agencies, tribal, state and local governments, cooperatives, and municipalities, collectively referred to here as “BESS Consumers,” as highlighted in Figure 1. Throughout this guide, the term BESS is used as the primary example for the target devices under consideration, but users can substitute other related terms with appropriate consideration for modifications that may be needed based on the technology or service being provided. This publication is part of the broader INL suite of publications and resources to support the industry in efforts to improve supply chain risk mitigation and overall energy security.

This BESS Procurement Guide is part of a series of INL publications and supporting initiatives focused on enhancing BESS cybersecurity. For additional information on INL Digital Assurance project initiatives and other available resources, visit the [Center for Securing the Digital Energy Transition](#).

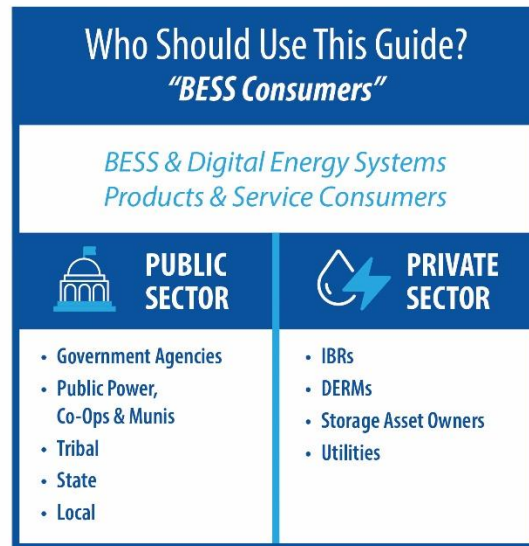


Figure 1: Intended audience for the BESS Procurement Guide.

1.2. Purpose

The BESS Procurement Guide's primary objective is to provide comprehensive guidance, informed by industry best practices to BESS consumers on how to incorporate cybersecurity requirements into the procurement process to enhance both BESS supply-chain security *and* entity-specific supply-chain risk management-(SCRM) programs. Many organizations procuring BESS equipment and services either: (a) do not have internal programs to mitigate cybersecurity supply-chain risk, (b) have programs that are still at an early maturity level, or (c) have programs that do not account for the industry-wide lack of mature cybersecurity in BESS. However, the significance of the risks to critical infrastructure as these technologies are integrated, and the pace of escalation across the cyber threat landscape, require that BESS cybersecurity SCRM programs more-rapidly mature than they might in a less-dynamic and lower-risk environment.

This publication will help BESS consumers and other entities integrating digital energy infrastructure, to accomplish the task of quickly, developing and maturing cybersecurity SCRM programs and maximize their ability to manage non-domestic equipment appropriately. While a comprehensive SCRM program is recommended, **given the criticality of implementing immediate controls, three critical foundational elements are presented for focus** in this guide to help prioritize the procurement processes that would mitigate many of the highest-consequence supply chain cybersecurity risks:

- **BESS Vendor Request for Proposal (RFP) and Solicitation Requirements** include bid-process requirement recommendations to improve bid and selection processes and reduce lags in risk assessment and procurement-agreement timeline once security requirements are integrated
- **BESS Vendor Risk Assessment** contains a basic risk analysis and impact factors, decision trees for initial evaluation, and risk-assessment methodology guidelines
- **BESS Procurement Agreement Terms** provide sample terms and conditions for vendor agreements to mitigate security and supply-chain risks associated with procurement of digital assets and services, including software and hardware bill of materials requirements.

1.3. Trends in Supply-Chain Cybersecurity Policy

In the last 3 years, a marked increase in focus is seen on supply-chain security by governments across the globe. Some of this is driven by rising geopolitical tensions, increased threats from nation states, and expanding reliance on digital technology in the operation of critical infrastructure. Much of it is also driven by a recognition of the need for a rapid maturation of cybersecurity and supply-chain risk mitigation to counter the risks presented by these factors, along with the rising digitization of key critical-infrastructure technologies like BESS. This state is depicted in Figure 2. The recognition of these risks has resulted in the issuance of policy guidance by governments, agencies, and industry standards boards, along with enhanced security standards frameworks and expanded regulation to better drive the prioritization of that maturity across every aspect of the supply chain (from suppliers through to end users). Leading this trend was the issuance of the North American Electric Reliability Corporation's (NERC's) CIP-013 regulatory standard, effective in 2020, that regulates cyber SCRM for the bulk-power system [2]. Another example can be found in the European Network and Information Security Agency's (ENISA's) focus on the topic and in its published series providing guidance on cybersecurity SCRM within the European Union [3].

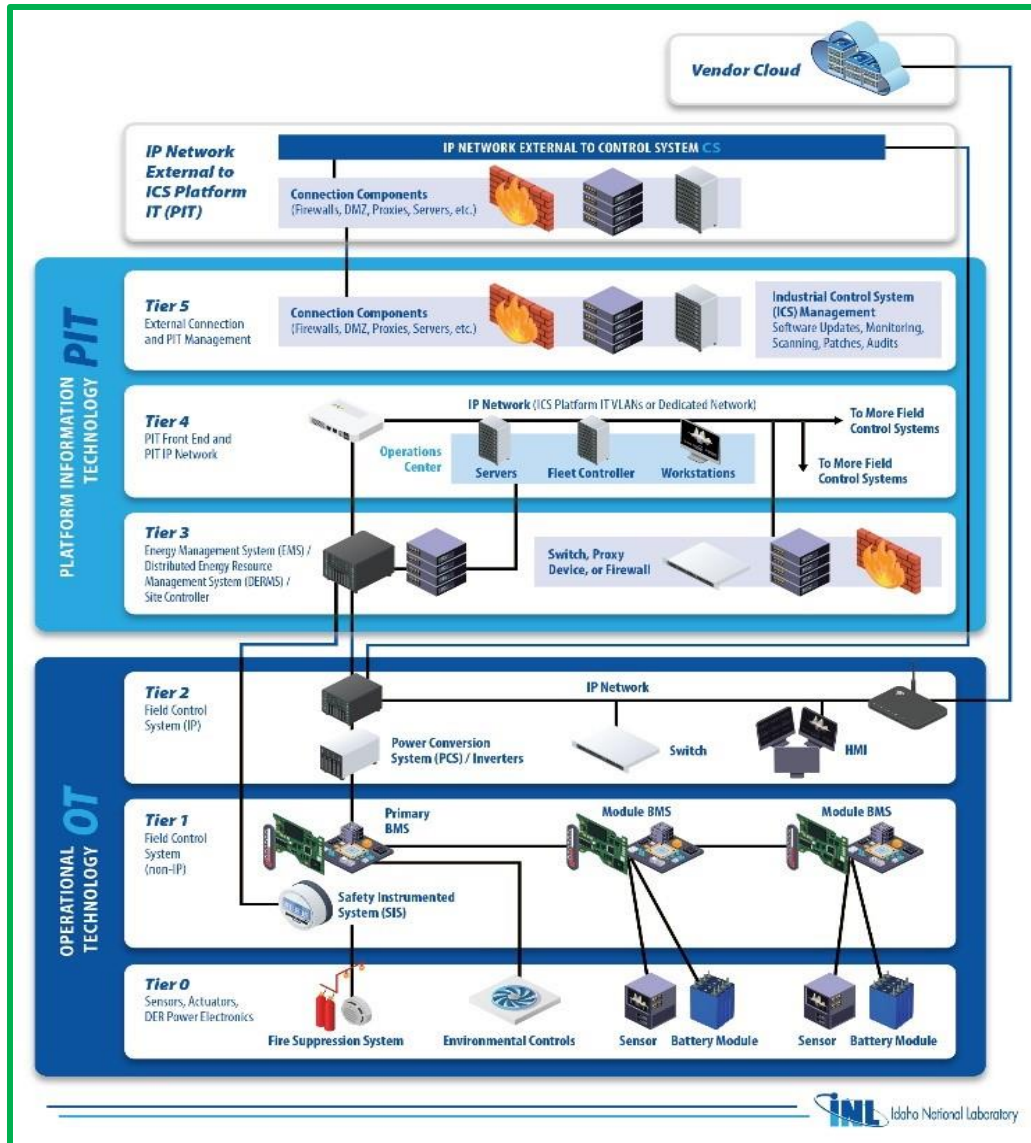


Figure 2: The Purdue model represents BESS, highlighting the connectivity and digitization of energy assets increasingly relied upon for grid stability and reliability.

Another key example of this increased focus and prioritization is illustrated in the recent issuance by the DOE of the Supply Chain Cybersecurity Principles [4]. These are a framework of critical foundational activities needed to support better industrial control system (ICS) security (refer to Figure 3).

In developing these principles, the United States is issuing a collective call to action for ICS suppliers and end users across the globe to support and adopt the principles. The principles characterize the best practices that are exhibited today by cybersecurity leaders in the energy industry and can help to create shared expectations that ripple throughout the supply chain, informing and lifting up manufacturers and owners and operators with less mature supply chain risk management efforts [4].

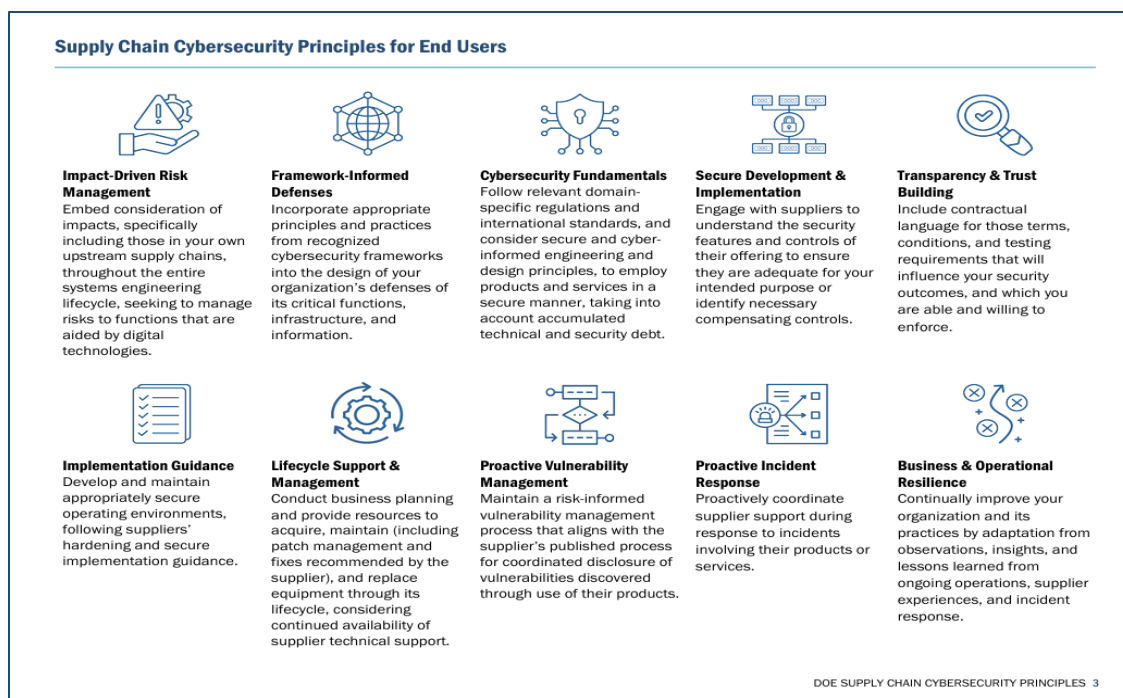


Figure 3: DOE supply-chain cybersecurity principles. [5]

With this increased attention and call to action, DOE engaged several major suppliers to support industry efforts to mature supply-chain security. DOE has funded initiatives like this one to guide everyone working to develop SCRM programs in implementing these principles. These principles also provide a baseline that procurement and contracting functions can consider in evaluating companies, products, and services.

1.4. Introduction to Battery Energy Storage Systems and Inverter-Based Resources Supply-Chain Security

As noted above, BESS, IBR, and other energy-sector digital equipment can present—indeed, are perceived to present—security risks due to the nature of their architectures: persistent communications, organizational challenges with foreign ownership, and unknown spiderwebs of components. As seen in Figure 4, a BESS supplier could provide battery packs that may have cells or modules from another vendor. That vendor could be providing their own battery-management system (BMS) or integrating that of a third supplier. Similarly, the power conversion system (PCS) and inverter could be from one that the company already involved or others entirely. Adding to these challenges, the landscape of BESS providers rapidly changes, with mergers, acquisitions, and dissolutions that may affect the named brand, manufacturing location, design, or assembly of components. Many of these risks can be reduced and mitigated with SCRM that focuses on procurement processes and contract terms. This publication provides that guidance.

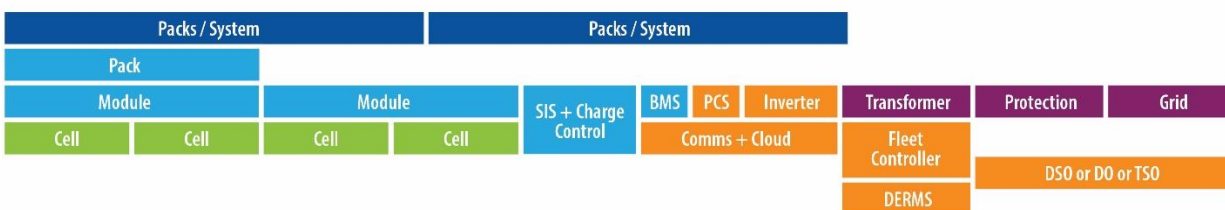


Figure 4: BESS components and potential vendors.

Organizations that integrate SCRM considerations as part of procurement guidance can mitigate supply-chain risks from the start, rather than addressing the rapidly ballooning challenge of identifying all components, all sources of components, and the known vulnerabilities and exploitability of existing equipment for both software and hardware, simultaneously. Well designed guidance should focus on eliminating risk as well as introduce risk transferal, requiring other stakeholders to take on some of the responsibilities for ensuring security of components throughout their life cycles. Below are some critical risk factors specific to BESS that should be part of any provided guidance and program addressing BESS supply chain security.

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

- Remote monitoring and control capabilities, expanding adversary attack surface
- Remote software and firmware update capabilities, which can allow suppliers to quickly deploy patches, but also expose 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 can be introduced at multiple points of the production process:

- Design, procurement of subcomponents (e.g., processing chips), manufacturing, assembly, and shipping.

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

- Less regulation or oversight of the design and manufacturing process, which may allow lower-quality manufacturing or design to slip through
- 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 proprietary information about equipment that could be used to plan adversarial action against the end users.

2. MATURING BESS SUPPLY-CHAIN CYBERSECURITY: GENERAL OVERVIEW

2.1. Introduction to Cybersecurity SCRM Programs

Implementing a SCRM cybersecurity program can be a daunting endeavor for any organization. The escalation of cybersecurity attacks and threats against both renewable and traditional power infrastructure and expansion of the landscape, particularly within critical infrastructure, has necessitated an immediate focus on the development of SCRM cybersecurity programs. BESS systems are no exception. In fact, as discussed above, BESS introduce increased security risks to power sector infrastructure both because of their critical role in the transition to a grid of the future and the high percentage of reliance on foreign-sourced supply chains.

While the importance of addressing these risks and implementing a strong program may be understood, putting a mature SCRM cybersecurity program in place is typically a comprehensive and long-term undertaking. This program guide **supports an ability to enhance SCRM while enabling the integration to proceed without burdening the owner or procurement organization to a no-go point.**

Before moving to the detailed recommendations for critical elements, which are the focus for this BESS Procurement guide, it is helpful to understand, first, how those elements fit within a mature well-designed SCRM cybersecurity program. Like many enterprise-level controls programs, most entities tend to structure them with two core components:

1. **Program.** This is an overarching enterprise level program (typically documented) that provides the basic objectives, communicates the organizational purpose and policy behind the program, defines core responsibilities, sets minimum program expectations, and mandates a structure for overall SCRM program governance, management, and compliance.
2. **Implementing or Executing Controls.** These are all the business-line processes and controls that will support the implementation of the enterprise supply chain risk management program at every level. Figure 5 below provides a basic overview of a typical SCRM program architecture.

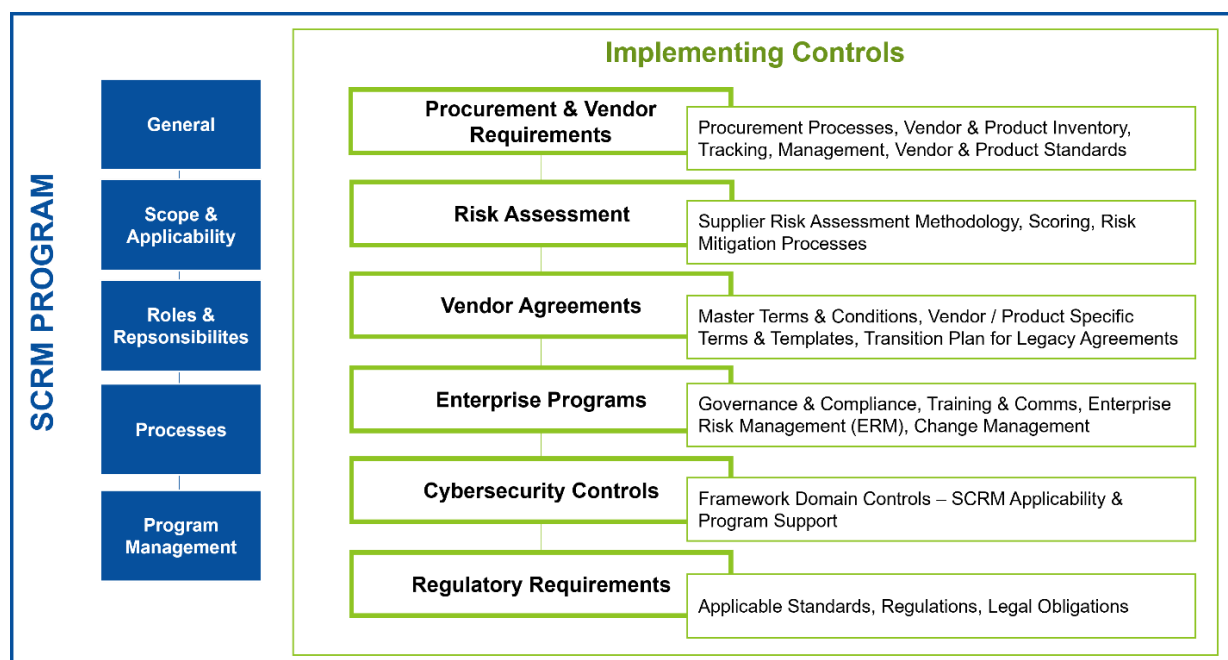


Figure 5: Framework for SCRM program architecture with examples of implementing controls.

Understanding most entities will not have the capability to immediately develop a robust SCRM program for their BESS, IBR, and other digital systems and equipment, this BESS Procurement Guide focuses on the most critical elements: Procurement and Vendor Requirements; Risk Assessment; and Vendor Agreements. Focusing on these, as seen in Figure 6, will help BESS Consumers rapidly adopting digital equipment quickly close the typically higher priority security risk gaps

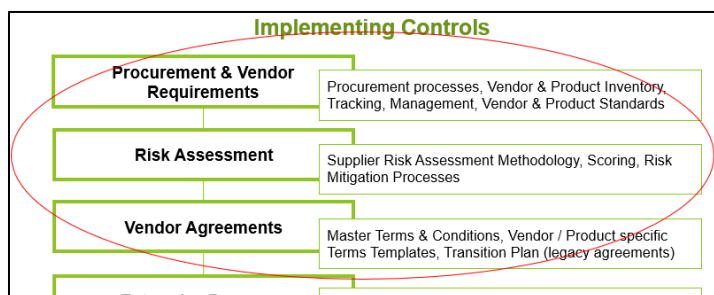


Figure 6: This BESS Procurement Guide focuses on prioritized SCRM program elements: procurement and vendor requirements, risk assessment; and vendor agreements.

Legacy vs New Suppliers. A final basics note. Many organizations will need to take a different approach for applying any new SCRM program requirements to existing vendors. Existing agreement terms may not permit or limit: (a) the adoption of new requirements, (b) certain critical activities included in the new program, and/or (c) the application of stringent security requirements. This should be a consideration for the critical elements discussed below as well. The most common approach is to split the implementation efforts and apply the new processes and controls to all vendors going forward, then establish an initiative to identify high-risk existing vendors and evaluate an approach for these on a case-by-case basis.

2.2. 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 to ensure suppliers have also prioritized security.

Development of key controls focused on communication of minimum standards as part of the bidding and selection process for a defined set of products and services vendors (e.g., any vendors associated with critical and high-risk digital components), intake analysis guidelines to determine whether and what type of risk assessment may be required, and a formal risk-assessment methodology for vendors that are selected to provide products and services included in the defined vendor set are an excellent start to driving those cybersecurity supply-chain objectives. Each of these is discussed in more detail below.

Figure 7 provides an overview of a typical, basic maturity approach. This BESS Procurement Guide focuses on recommendations for the procurement process (Items 1–3), discussed in detail below. Item 4, supplier management, covers the ongoing process to monitor for continuous compliance after procurement has occurred. Future guidance will cover that topic in greater detail.

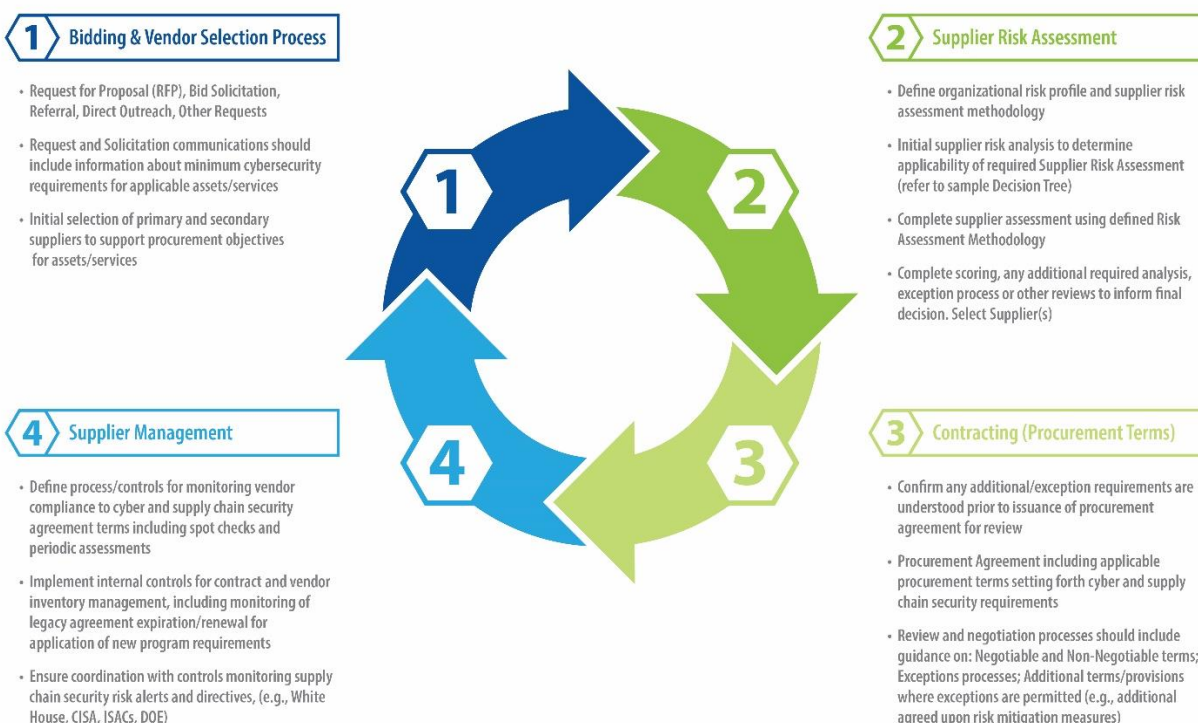


Figure 7: Basic cybersecurity guidance for a SCRM procurement program.

3. MATURING BESS CYBER SUPPLY CHAIN SECURITY: PROCUREMENT BIDDING AND SELECTION PROCESSES

3.1. Vendor Selection Processes

Bidding, request for proposal (RFP), vendor solicitation, direct outreach, and other processes for the identification and selection of a BESS supplier should be updated to include minimum expectations for supply-chain and cybersecurity. Doing so will help potential suppliers understand whether they will be able to meet their obligations should they be awarded the contract and will save the procurement function and interested internal buyers time and effort. These requirements may be added to initial communications, RFP and solicitation documents, frequently asked questions (FAQs) and other bid-process materials as well as any supplier-facing general brochures and program guidelines.

The nature and extent of what is included is usually informed by the cybersecurity procurement-agreement terms and conditions (see Sample Procurement Agreement Terms). Key considerations include:

- **Initial and outreach communications** should include a high-level summary of applicable supply chain-security and cybersecurity requirements tailored to the BESS product or service security needs.
- **RFP and Formal Bid/Solicitation Requests** should include an outline of the requirements and detailed summary of any that may be more restrictive. The amount of information needed will vary depending on the target audience. Vendors that will provide what is considered higher-risk products and services should be given more information to ensure they understand the expectations and can consider the impact to the planned bid.
- **General supplier program brochures and guidelines** may include a statement about the organizational commitment to security, a summary of requirements applied, and expectations for suppliers.

3.2. Vendor Inventory and Management Controls

Any procurement initiative to manage vendors requires a comprehensive inventory of all suppliers. For organizations that do not already have this in place, a risk-based approach to developing this supplier inventory will ensure at least a focus on identifying energy-sector digital-equipment suppliers that pose higher cybersecurity risks to the organization. The procurement function should prioritize developing a complete inventory and a process for maintaining it. Examples of data points to include are:

***Reminder:** Periodic monitoring/triggering event controls—e.g., notice of pending end of contract—should also be developed to ensure the inventory is properly managed and kept current.*

- Supplier type (product/services)
- Basic demographic information, to include name history—e.g., mergers and acquisitions
- Ownership and key location data—e.g., foreign ownership
- Locations of U.S. offices, relationships in the U.S.
- Indicators of any high-risk regions, sanctioned countries, and controls to monitor or flag
- Product-manufacturing locations
- Shipping and assembling locations
- Risk classification or designation (based on organizational risk assessment)
- Presence on allow lists or banned and sanctioned lists
- Subcontractor relationships and data

- Agreement start and end dates
- Key contacts
- Software bill of materials (SBOM)- and hardware bill of materials (HBOM)-requirement indicators and component tracking; where available and provided, this additional detail should be integrated at a high level to provide quick view transparency to the supplier products
- Temporary or persistent access to systems (e.g., manufacturer asset-health monitoring).

4. MATURING BESS SUPPLY-CHAIN CYBERSECURITY: VENDOR RISK ASSESSMENT

4.1. Organizational Risk Overview

Before diving into the specifics of vendor screening and risk assessment, it is worth reviewing basics on organizational risk that will inform and must be incorporated as a part of specific SCRM controls. Organizational-risk management is typically an enterprise-level task, integrating all risks as part of a developing organizational risk-assessment process. This process begins with an understanding that there is no one-size-fits-all model or template. How risk considerations are defined, and what risks may be tolerable, is unique to each organization. Before defining a *supplier cyber risk-assessment process and methodology*, the organization should first ensure an understanding of the broader-enterprise risk priorities, business-risk tolerance, and supply-chain and cybersecurity risk-management objectives.

4.2. Defining Organizational Cybersecurity-Risk Assessment Priorities for BESS, IBR, Energy Digital-Equipment Products and Services

Organizational-risk management is typically an enterprise-level task, integrating all risks as part of an enterprise-risk management (ERM) program. These tend to focus on corporate and traditional—e.g., financial, operational, legal—risks. Supply-chain and cybersecurity risks are a newer domains for inclusion in ERM programs and are not yet standardized, making them more difficult to assess and measure. It will be necessary to understand the enterprise-risk model to inform the design and implementation of a risk-based SCRM program.

BESS supply-chain cybersecurity risks should be a component of the enterprise program, probably a subordinate element of cybersecurity-risk analysis, and defining these may be simpler than defining the broader cybersecurity-risk domain.

Because the organizational supplier-risk-assessment methodology will likely be applicable for a much broader use than just BESS product and services suppliers, before moving to the more-specific BESS risks, it will be helpful to keep the broader cybersecurity and supply-chain risk domains in mind as well. At a high-level, these are:

- **Cybersecurity Risk.** Risks raised by vulnerabilities and threats to hardware, firmware, software, technology products or tools used to operate organizational assets and manage business information or data. These risks may be presented by external threats or vulnerabilities, may also be caused by gaps within the organizational processes and controls used to protect these assets, by personnel implementing security controls or even by security-mitigation measures. For example, a failure associated with a patch-management process could also be a cybersecurity risk.
- **Supply-Chain Risks.** Risks that exist within the supply chain of products and services an organization may procure. These risks may exist *before* the products are introduced into the organizational environment or may become or remain a risk within the environment once an asset or service is procured. Supply-chain risks may be cybersecurity risks or other product and vendor risks, such as the inability to procure equipment due to manufacturing problems within the supply chain, changes to subcomponent designs or prices or to supplier organizations. Supply-chain risks are often discussed as “Tier 1, 2, 3 . . .” and so on to indicate how far removed from the supplier the purchasing organization may be. This is important to the level of transparency the purchaser may have and legal rights available if there is no contractual relationship with the tiers further down the supply chain.
- **Supply Chain Cybersecurity Risk.** These are *cybersecurity* risks that are introduced into an organizational environment via the supply chain. Risks to enterprise operations and assets that may arise due to supply-chain risks (Tier 1 through sub-tier suppliers) introduced by vendors providing cybersecurity-related products, equipment with cybersecurity-related operations or capabilities included, or in the provision of services. Supply-chain cybersecurity risk can be seen as a subset of both cybersecurity risk and supply-chain risk. Where it will be managed within the company, from an ERM perspective, depends on the organization.

These are all foundational broad cybersecurity-risk elements that inform the supply-chain and cybersecurity-risk assessment processes and methodology.

4.3. BESS Supply-Chain Cybersecurity Risk Considerations

In addition to the broader organizational and supply-chain and cybersecurity risk considerations that are foundational to a good general SCRM methodology, critical considerations specific to BESS, IBR, and energy digital-equipment supply-chain cybersecurity risks may include:

- **Programmable and Remote Operability.** What remote operations and control capabilities exist in the BESS? Remote connectivity is not a negative feature on its own; in many cases, it is required to allow BESSs to achieve all their intended functionalities. However, organizations should be aware of all the interfaces, protocols, and access ports that grant remote access to the device and what operations can be carried out through those channels. Can system configurations be changed? Do all channels require authentication?

- **Access-Management Controls.** Are there strong access-management controls for all personnel with privileges, including provisioning, timely deprovisioning (within 24 hours for terminations), background checks, monitoring for changes in vendor personnel, defined least-privilege tiers, and frequent periodic reviews?
 - **Vendor Access to Devices.** Many BESS and IBR providers build features that allow them to have persistent remote access to the devices after they are installed and commissioned. They may want or need access to data to perform asset-health monitoring or collect data that may help them improve designs of future releases. Many vendors also use remote connections to push firmware and software updates to their devices. There are tradeoffs with this approach. Direct access allows vendors to rapidly push critical patches to devices that might affect performance or security without relying on customers. However, cutting the customer out of that process prevents the customer from being able to test and validate that a patch does not have any adverse effects in their environment before deploying it to all field systems. Additionally, as seen with the 2024 CrowdStrike incident, errors in updates can cause widespread impact if deployed to all systems simultaneously. Many vendors will try to **build persistent-access requirements into their sales contracts**, stating that warranties and service agreements will be voided if the BESS consumer blocks the vendor's remote access. Recommendations in this document provides some alternatives to limit the risk of vendor access to devices through procurement terms.
- **Power-Conversion System (PCS).** The PCS is the component in a BESS that performs conversion of energy from alternating current (AC) to direct current (DC) and vice versa, depending on whether the battery is charging or discharging. The PCS is responsible for coordination of power and control, and it manages the communication from internal to external components. This component is significant because it contains many of the control features central to battery operation and grid support and manages communications. It has the potential to create high consequences if mis-operated, and it cannot be operated in isolation (i.e., it must maintain connectivity). Due to its criticality, it is worth paying particular attention to the supplier and manufacturing source of the PCS as part of SCRM considerations.
- **Foreign-Sourced Products and Services.** Where is the supplier located? Where are they headquartered? Do they have U.S. offices? Are they owned by a larger conglomerate? Are they subject or susceptible to control or other obligations by a government or other third party? Company headquarters can be an indicator of threat due to the laws in those countries that may compel the companies or individual employees to act against U.S. national-security interests. Are there possible incentives by the product or services vendor to disregard security risks due to the supplier's location (e.g., the vendor does not adhere to risk guidance issued by the U.S.)? This question can be made more complicated by complex and ever-evolving mergers and acquisitions, renaming of companies, or other business mechanisms that make it difficult to determine who is actually driving decision making.
- **Country of Origin Risk.** Where is the product manufactured and assembled? This may be several locations depending on the manufacturing process for the device. The source of components can be an indicator of threat. Vendors that manufacture in or source components from a country labeled as a geopolitical cyberthreat present a higher risk.

Manufacturing location and company affiliation should be considered jointly. For example, there is a growing trend of Chinese companies manufacturing products in Mexico to avoid tariffs and sanctions against China because the goods would be considered to be Mexican in origin [5]. Conversely, leading inverter producers headquartered in the United States and Israel have production facilities around the world, including China, Mexico, Hungary, and Vietnam. Even when inverters are designed and assembled in the United States, the application-specific integrated circuits and semiconductor power-handling components are almost entirely produced in Asia [6].

- **Lack of Supply Chain Transparency.** The landscape of BESS companies is large and always changing. Inverter companies change their names, undergo mergers and acquisitions, or shut down frequently. Some of this is due to the dynamic nature of the solar-photovoltaics market, but some of these changes are also related to companies trying to get around certain regulations. For example, a foreign company in what has been designated by the Federal Government as a “high security risk” region may choose to sell their products within the U.S. under different names to bypass or evade associated limitations. In addition to the challenge of tracking these changes and understanding the complex organizational structure of some of these companies, it can be difficult to track where subcomponents originate, especially on the digital side. Identifying all of the libraries required for a piece of software to run, let alone the source of all those libraries, may be prohibitively time consuming, particularly for an end user. Controls to specifically address this risk should be considered for inclusions, such as more-rigorous testing, analysis, and pre-deployment segmentation requirements for high-risk equipment, use of enhanced cybersecurity monitoring and mitigation controls (e.g., internal-network monitoring and targeted escalation protocols).
- **Whitelisting.** Is the supplier and/or the particular device present on state or federal allow lists? Conversely, is the supplier on any federal sanctioning or ban lists? Presence on allow lists can indicate some level of vetting and approval has been done. Presence on sanctioned or ban lists may or may not indicate there are cyber risks associated with the supplier, but that there is some risk introduced by the supplier. Even if the identified risk is acceptable to an organization, presence on ban lists may indicate that it could be more difficult to work with these suppliers as they navigate the regulatory hurdles.

In addition to including these risk considerations as part of enhancements to SCRM procurement processes, specific contract terms can be developed to address these. However, contract terms primarily shift risk and liability in the event something occurs, and while this may be a good deterrent, it will not prevent a major security event; thus, it should not be the only risk mitigation measure.

4.4. BESS Vendor Intake: Initial Screening, Analysis, Risk Assessment and Exception Processes

Not all BESS suppliers present the same level of risk to the organization, so until the program is mature, entities will likely try to limit the volume of risk assessments to higher-risk procurements. Conducting an initial analysis to determine whether and what type of risk assessment may be necessary will allow for better risk-based prioritization of vendors requiring assessment and will reduce delays in procurement-process and agreement timelines. Organizations should develop an initial intake-analysis process to facilitate a standardized approach. The sample decision trees in Section 4.4.1 for products or equipment and services provide some guidance. Organizational enterprise cybersecurity and supply-chain risks (discussed above) should also be considered when defining one specific to the entity program.

Developing a standardized intake-analysis process to prioritize which vendors to assess will support a risk-based approach and reduce impact to internal resources of new program implementation.

Existing/Legacy Suppliers Note. Organizations looking to apply the program to legacy assets and existing suppliers may want to develop a decision-tree model specific to those types of assets that allows for the ability to better prioritize an initiative to address existing high-risk suppliers.

Less-mature programs should include the ability to begin with something like this decision-tree approach to first determine which suppliers will be subject to the risk assessment, then move to applying the risk-assessment methodology (sample provided in the next section).

4.4.1. Sample Decision Tree for Initial Analysis of Service Suppliers

Figure 8, below, is an example of how the determination that the full risk-assessment methodology must be applied to a services supplier might look for an organization.

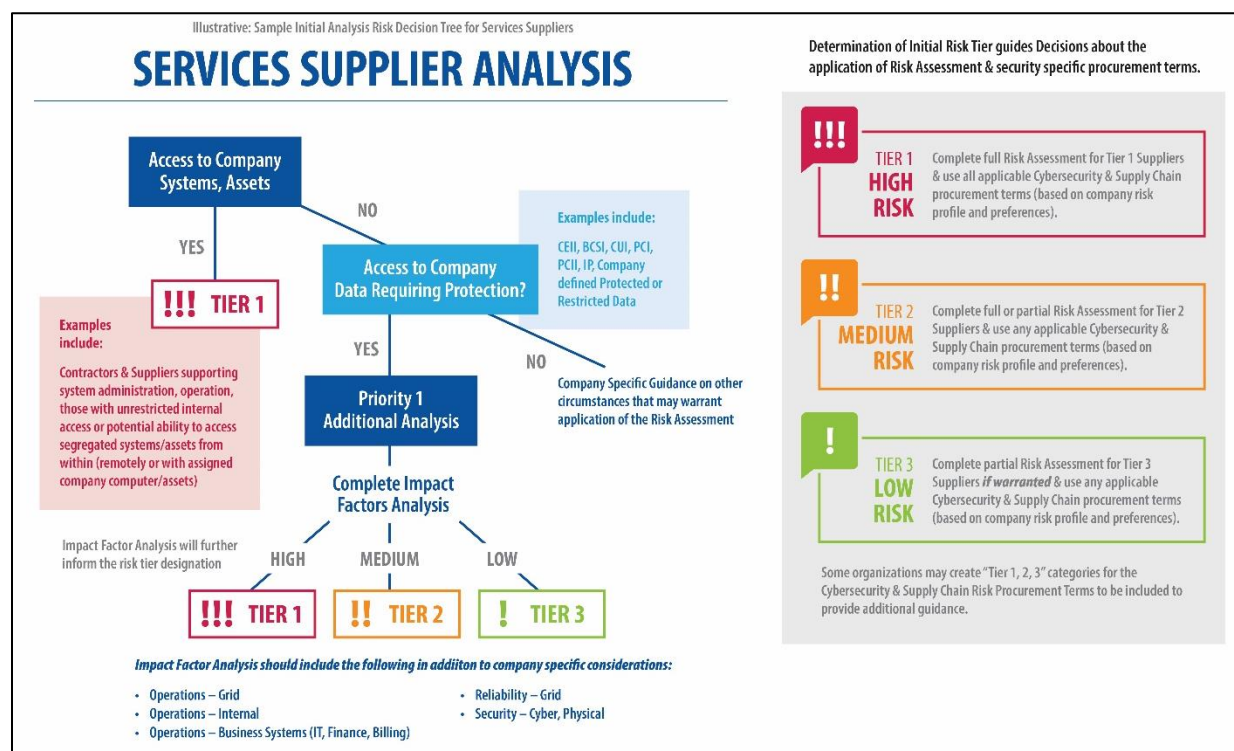


Figure 8: Sample initial-analysis risk decision tree for service suppliers.

Examples of classifications of BESS service suppliers:

- **Tier 1:** A BESS maintenance provider that maintains persistent access to the systems to provide health monitoring and proactive maintenance services. This may be the same company that manufactured or installed the BESS.
- **Tier 2:** A developer that installs and commissions the BESS system. The developer has significant access to the BESS system during construction and commissioning and works with the BESS consumer to integrate the BESS into the larger system, which may give them temporary access to company systems or assets.
- **Tier 3:** A maintenance provider that visits onsite periodically, or as required, to inspect electrical systems for safety hazards or provide maintenance or repairs. The contractor is escorted on site and uses organization-supplied computing resources (i.e., an engineering laptop) when onsite, so no new devices are introduced to the environment, and no data leave the environment.

4.4.2. Sample Decision Tree for Initial Analysis of Products, Assets, and Equipment Suppliers

Figure 9 shows an example of how the determination that the full risk-assessment methodology must be applied to a product supplier, including hardware, software, and other equipment, and how that might look for a particular organization.

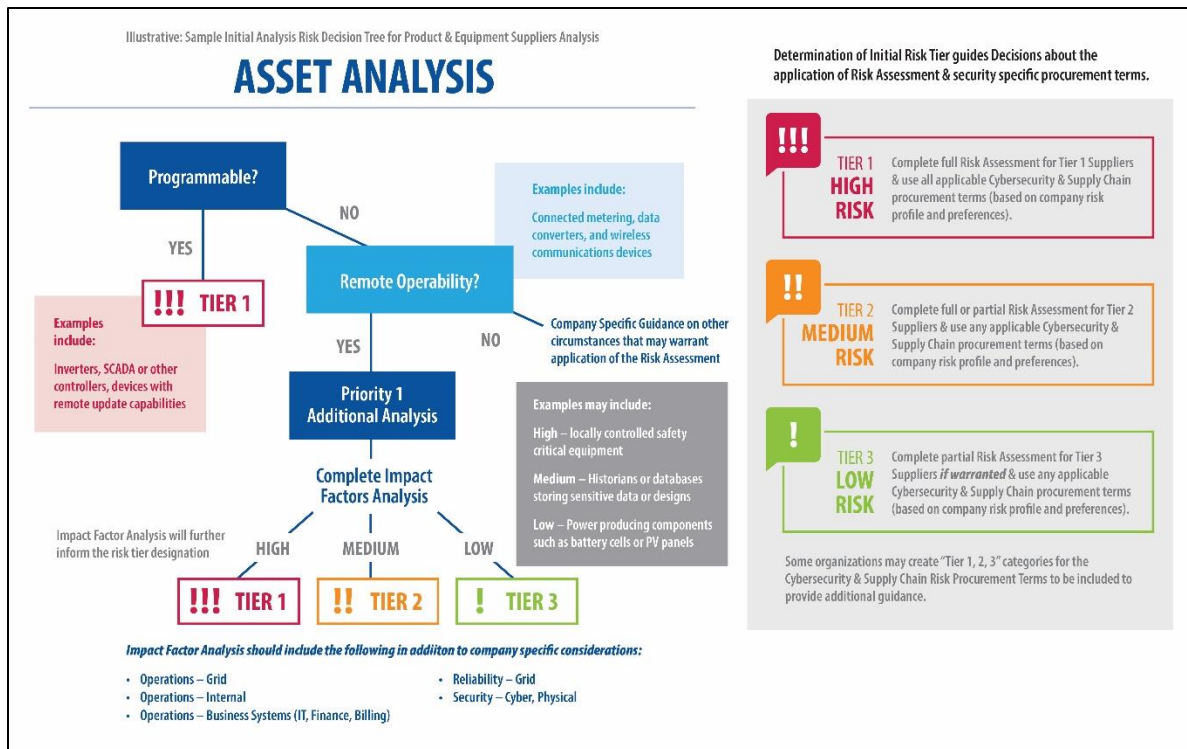


Figure 9: Sample decision tree for initial analysis of products, assets, equipment, or suppliers.

4.4.3. Out-of-Process Procurements and Exceptions

All SCRM programs should include guidance for how to manage out-of-process procurements and exceptions. These situations will be inevitable; it will be important to ensure teams understand when it is permissible and that these processes should not be overused. If out-of-process procurement of products and services is permitted, all procurement and risk-assessment guidance will need to be updated to reflect where this is **not** allowed or what approvals may be required for certain supplier products and services. The procurement asset inventory process should also include a review to identify potentially missed procurement activities that should have been subject to the full process controls. Where a procurement department has allowed for procurement process deviations for certain products and services (e.g., emergency, low value, work orders), these should be reviewed to determine whether they need to be updated to reflect the organizational risk tolerance specific to BESS suppliers.

This is also a good area within the program for use of a defined quality assurance (QA) control and a defined metric. For example, a metric to track how often out-of-process procurements occur and exceptions are granted, and quality-assurance controls to spot-check use of the process as well as periodically review exceptions and reevaluate whether the circumstances supporting the exception warrant continued applicability.

Exceptions to the procurement requirements for vendors who are subject to the full risk assessment are discussed in the next section.

4.5. BESS Vendor Cybersecurity Risk-Assessment Methodology

Once the consumer has completed the initial intake analysis and determined a risk assessment should be initiated for BESS assets and/or services providers, it will need to conduct the risk assessment in accordance with the entity-specific risk-assessment methodology, which should provide guidance for how to use it based on the initial intake-analysis designation. For most entities, once it is decided a risk assessment is required, the designation will mostly inform whether exceptions or out-of-process procurements are permissible, that may factor into the scoring and/or may influence whether additional discretionary decision making requires approvals at various levels.

Figure 10 is an overview of the major supplier risk-assessment activities where an assessment will be conducted. The discussion that follows provides helpful guidance for developing these components of the procurement processes.



Figure 10: BESS vendor cybersecurity risk-assessment methodology summary.

4.5.1. General Considerations for Assessment Methodology/Process

The scope and applicability of a formal supply-chain risk-assessment methodology will be heavily informed by: (a) the risks the organization is attempting to mitigate with the assessment, (b) the entity specific risk profile, (c) the approach to enterprise risk and risk tolerances, and (d) a variety of other organizational factors. It may also be influenced by external regulatory and operational obligations. These should all be considered as part of the development of the formal methodology.

When an organization is developing their individualized risk-assessment methodology, in addition to the key actions for completion of the supplier evaluation (outlined in Figure 11), a few additional key considerations might be included in the process:

- **Purpose.** Ensure the company objectives are clearly stated within the purpose specific to cybersecurity supply-chain risk management and highlight critical risk objectives related to BESS services and assets.
- **Regulation and Legal Requirements.** As regulatory requirements begin to expand, the risk-assessment methodology should include guidance on applicable regulations and other legal obligations, as well as a control for verification and updates to these obligations. For BESS-related assets, for example, NERC and state commissions regulating distribution-level assets are working to expand requirements to mitigate risks introduced to bulk-power and other grid assets.
- **Scope and Applicability.** The scope should provide sufficient guidance for some discretionary considerations but should also define types of assets to be specifically included. In addition to general categories—e.g., hardware, firmware, software, services—specific assets and service types may warrant inclusion and additional details and guidance. For example, for BESS-specific program applicability, an entity might include:
 - BESS (with subcomponents often included as a package):
 - Battery cells, modules, packs
 - BMS
 - PCS
 - Environmental controls (e.g., fire protection)
 - Skids and racks
 - Human/machine interface
 - Site controller and/or fleet controller (depending on scale)
 - Supervisory control and data acquisition (SCADA)
 - Metering
 - Protection (relays and breakers)
 - Distributed energy-resource management system and/or energy-management system (depending on scale)
 - Engineering, procurement, and construction services
 - Developer services
 - Integrator services
 - Network monitoring services.

Applicability will depend on what the organization prioritizes as being in scope and mandatory vs discretionary for inclusion. Sample language might be something like:

This methodology is **mandatory** when procuring [asset/service types] defined in the Scope section and should be considered for application to procurements of other systems and services as a good

business practice. This methodology does not apply to the procurement of [items that may be excluded, e.g., devices, equipment, supplies, that are not programmable, such as power poles, office supplies, building construction supplies].

- **Restrictions on Use of Payment Card or Invoice Purchases.** Consider whether there should be any limitations or requirements where payment cards or direct invoices (not requiring procurement agreement or processes) may be used for in-scope assets. This may make it difficult to ensure the controls are executed for procurements that must be considered for assessment and SCRM procurement terms.
- **Enterprise Architecture and the “No One-Size-Fits-All” Challenge.** Finally, a critical consideration for small business, independent contractors and other non-standard larger organization enterprise models. As supply-chain security programs have matured and third-party risk becomes an expanded and critical risk of focus for many organizations, many have begun applying the programs more broadly to include most suppliers. However, most programs and assessment models are designed with the assumption of a single basic architecture. Many small businesses do not fit within this model.

For example, many independent contractors (typically service providers) do not use enterprise-architecture models or even third-party services. They may just be using a personal computer with an instance of Microsoft Office 365 and a few applications. No access-management controls, vulnerability assessments, or other typical cybersecurity-domain processes in the manner typical of assessment models affect that system. None of these are needed to effectively mitigate risk either.

When developing the organizational SCRM program, taking the time to more-thoughtfully consider alternative vendor infrastructures, architectures, and other security models will help ensure possible inclusion of guidance on how to apply the procurement processes and risk assessment methodology where these distinctions exist. Doing so will substantially reduce the amount of time to address each individually as questions arise, while allowing for consistent execution where required to mitigate risk.

4.5.2. Completing the Vendor Evaluation

As discussed above, several key activities are recommended to complete a vendor-evaluation process. Key considerations for each can be used to inform and design an entity-specific methodology that closely fits an organization (see Figure 11). Each should be included in a documented process that provides clear guidance to the internal teams responsible for conducting assessments.



Figure 11: Three major steps to complete a vendor evaluation.

1. Collect the Necessary Vendor Information and Assess Gaps

To begin the risk-assessment process, key information about the prospective supplier that will inform the assessment and scoring activities must be collected.

It may be helpful to put some tools and templates in place as well, such as spreadsheets provided to suppliers, a database tool into which to put that information, any selection of other templates, guides and tools and/or some combination. For some entities, an assessment vendor may be selected to help define this process and manage the initial assessment, data collection, and risk evaluation.

Vendor information and needed inputs will be informed by entity-specific risk factors, risk scoring criteria considerations, scope, and applicability, among other unique factors. If an assessment vendor is used, it is important to review that vendor's process, questionnaires, and data-collection set to ensure it is aligned to the entity-specific risk profile and, if not, to adjust it. Some ideas for what types of data might be critical to obtain and that tend to apply within most organizations include:

- Current supplier information or updates to existing information (if possible, this information may be pre-populated for review and update).
- Basic demographic information, including any specific requirements for certain types of vendors. For BESS, IBR, and digital energy-equipment products and services, this should include data about foreign ownership and control, foreign sourcing, and manufacturing operations.
- Cyber and supply-chain security hygiene that would typically include standard assessment input and criteria data points across all computer domains (e.g., asset inventory and baseline, access management, networking and protocols, incident response, vulnerability management, information and data protection, governance and compliance). For supply-chain security this may also include requests for information about SBOM and HBOM processes, controls, and capabilities.

Consider whether the program will permit vendors to provide third-party security assessments and/or certifications in lieu of completing the organization specific requirements. For vendors that are able to provide a third-party assessment or certification, if permitted, the process should provide guidance to procurement, such as:

- The criteria for evaluating validity of the certification vendor and a list of any approved certification vendors should be defined in advance.
- If provided, the certificate(s) should be reviewed and the data in the external assessment input/aligned to the program criteria to assess whether there are gaps remaining. The assessment request might then be limited to those gap areas. *See also the Gap Analysis note below.*
- Small Business and Independent Contractor Models. Consider whether the assessment and information collection may look different for smaller organizational models and would require different templates and scoring criteria. Most assessment frameworks assume a corporate hierarchy and enterprise-information technology (IT) architecture that does not match that of these vendor types. For example, typical access-management-domain questions are not applicable where an independent contractor who is not managing access for anything beyond their own computers.

Data-Gap Analysis. Once a vendor has reviewed existing or prepopulated data and/or provided all required information, determine what supplier criteria may have been met and can be immediately scored, thereby limiting the amount of analysis required to only those areas remaining. For example, if the supplier has provided a currently valid and approved third-party supply-chain security certification, such as a cybersecurity-hygiene assessment, a valid SBOM or HBOM **and** the process defines an immediate assigned score for these; then only the areas that are not aligned to the entity-specific requirements would need assessment.

2. Conduct the Risk Assessment and Calculate the Score

Once the vendor data are received, they can be evaluated and scored to inform determinations for approval, additional risk-mitigation measures, and/or restrictions. The entity-specific risk-assessment methodology will need to include a scoring table or guidance and process for conducting the part of the assessment that aligns to the entity risk profile.

Typically, the evaluation criteria will involve (a) a set of criteria for each important element of the assessment (e.g., cybersecurity-hygiene questions and domains or impact and use of the product or asset) and (b) a method for calculating a final overall score that is an indicator of the type of risk presented and any additional mitigation or restrictions that should be considered.

The risk-assessment methodology should define risk criteria specific to the risk tolerance and requirements of the entity and should consider factors of import to the organization. For example, if the entity is primarily employing remote access and operability for critical assets, the risk is higher for any equipment or service vendor that can impact this capability so there may be a predetermined assignment of risk to these products and services. Another example is with equipment-specific criteria. There may be specific designations for BESS assets that are programmable, that permit remote access and operability or that are purchased from foreign sources.

Existing/Legacy Suppliers Note. *The approach for existing services, products, and equipment may warrant different risk-assessment criteria and scoring. The risk-assessment methodology should include this consideration and provide guidance to internal teams on any distinctions in approach that may be supported due to the legacy or historical relationship and/or any associated limitations.*

In developing the criteria, consider using a scale to score, which will be easier to use to then average or support an overall quantification. Most organizations use a scale of 1 to 5 for the risk range criteria, with 1 being minimal risk and 5 being high risk.

Pre-Determined Initial Scoring. Additional scoring criteria might include a predetermined initial score based on the type of vendor or asset (e.g., BESS, IBR assets/vendors). This might also be informed by the initial intake analysis designation. Whether additional scoring analysis is warranted may depend on this predetermined designation.

For example, when scoring an asset that will be purchased from a vendor that manufactures products in facilities located in high-risk regions, that cannot provide a valid and complete SBOM, and that will be used in high-risk, high-impact operations, these circumstances might warrant an automatic designation as high-risk. No further analysis would be needed. This does not mean the vendor cannot be used or the product cannot be purchased; rather, it indicates that the defined protocols for high-risk classifications would now automatically apply. These may require certain approvals, additional mitigation measures, or other restrictions.

Conversely the designation of an automatic low-risk indicator may either mean no further analysis is needed or that the product or service is then evaluated according to the all-other-assets criteria. This should all be considered and defined in the guidance in advance to streamline the process and support consistent execution, which is critical to success.

Below are some possible ideas for how to think about defining predetermined risk criteria to be used for BESSs, IBRs, or energy digital-equipment products and services, which are collectively referred to as BESS digital assets. Note the difference from Bulk Electric System (BES) cyber asset, which has a NERC-defined meaning. Criteria should be defined for both asset and service vendors. In the examples below, there are 5 levels, with 5 being a product or service that might present the highest risk.

Risk Level 5: *BESS* cyber asset with built-in remote connectivity capabilities—e.g. is or includes cellular modem, router, firewall—or with direct control over safety-critical systems or service vendors that will have administrative access to cyber assets or equipment.

Risk Level 4: *BESS* cyber asset with direct control over operation-critical systems—e.g., charge and discharge, grid services—or connectivity to external partners and service vendors that will have remote access to cyber assets or equipment.

Risk Level 3: *BESS* cyber asset with indirect control over operations or indirect connectivity to external partners—e.g., when the only communication path is through a monitored firewall)—service vendors that will have physical access to cyber assets or equipment.

Risk Level 2: *BESS* cyber asset with responsibility over monitoring and reporting systems, but without direct control functions or service vendors with temporary, limited, or monitored access to company systems or assets.

Risk Level 1: *BESS* cyber asset without routable connectivity for controls—e.g. local feedback control loops—service vendors with no access to company systems or assets.

All Other Assets. For any assets that do not fall into the predetermined asset or services designations, scoring would proceed based on the criteria defined more broadly and aligned to the entity risk profile. This should be developed and included within the process. Typically, a score would be assigned for each domain that the entity has chosen to include within its assessment process. For example:

- Company demographic information. This score will be based on information such as size, location, whether the vendor provides a product or services, the type of product or service, the vendor's experience level, and other factors in line with the entity's risks associated with this demographic information.
- Cybersecurity framework domains. This designates a score for each: access management, vulnerability management, governance).
- Supply-chain security. This designates a score for common elements of a program if they are not included with the cybersecurity framework domains.
- Additional Criteria. Other specific criteria should be defined for high-risk factors that may or may not be included in predeterminations. For example, inclusion may depend on the organizational specific risk tolerance, factors determined to be a priority, and/or the ERM program. These include:
 - Operations, manufacturing, or sourcing in high-risk regions (defined)
 - Ownership structures that present specific risks
 - Reliability or uptime metrics, especially for BESS to be used in critical applications
 - Interoperability (e.g. compatibility with different types of management systems; does the BESS Consumer have to use the management system offered by that vendor?)
 - Security incidents or known critical internal-controls failures related to the products or services
 - The vulnerability-disclosure process (whether the vendor has a process for responding to responsible disclosures or stated internal guidelines for patch timelines for discovered vulnerabilities)
 - Past performance.

3. Calculate the Score

Once initial scoring criteria are assigned for each of the defined criteria, the weighted risk score should be calculated and averaged for an overall risk-assessment score. This overall score should guide what remaining actions are needed. This must also be tailored to the entity-specific risk profile. What procurement provisions and cybersecurity requirements are required may also be informed by the risk score, with more rigorous cybersecurity, liability, and insurance requirements where there is a higher overall score. Additionally, for high-risk BESS cybersecurity assets and services, it is common that specific approval requirements would be defined (e.g., management through to a senior-leadership approval for the highest risk) and mitigation measures would be required for the vendor and entity.

4. Document Results and Additional Requirements

As noted above, prior to finalizing the determination and communicating this to the vendor:

- Identify and evaluate any final additional considerations that may impact determination. These may include any existing agreement terms with the vendor, availability of alternative vendors, level of expertise or capabilities vs. other vendors, and even the entity's ability to mitigate any risk posed by the vendor.
- Finalize any specific contract requirements, as well as risk-mitigation measures that may be required. These should be defined, documented, and communicated as a condition of the approval. These should also be included in any procurement-team tracking and vendor-inventory information to ensure an ability to effectively define oversight controls and verify compliance, where applicable.

Risk Mitigation Note. *It is not practical to mitigate every risk to zero. The objective should be to define requirements that allow for the mitigation of the risk to an acceptable level. It is common for risk-mitigation measures to be needed and requested. Consider any mitigation of risk to an acceptable level that may be necessary for approval of the procurement. If the vendor refuses to cooperate, ensure that the risks can be mitigated to an acceptable level before proceeding and that a process or guidance is defined in advance for making this determination. If the risk cannot be mitigated to an acceptable level, guidance should be included concerning any requirements to identify a different design or approach to the situation.*

4.5.3. Final Approvals, Selection Confirmation, Formal Agreement, and Vendor Communications

Once the risk-assessment process is completed, and vendor approval or denial is confirmed, these facts can be communicated to the vendor. Where the vendor is approved subject to additional agreement terms and/or risk mitigation measures, these should be included and clearly defined as a condition of approval. It may be helpful for the entity to have some understanding of where there is any negotiation room and have designated specific internal team members who will be primary leads for any negotiation of the terms *prior* to providing the requirements to the vendor.

Once finalized, the customer must ensure that any vendor-related tracking and inventory has been appropriately updated to reflect required supply-chain and cybersecurity terms and conditions.

5. MATURING BESS CYBER SUPPLY CHAIN SECURITY: VENDOR AGREEMENTS AND PROCUREMENT TERMS

5.1. Procurement Agreements

Procurement-agreement terms and conditions setting forth minimum supply-chain and cybersecurity requirements is an important control within the supply-chain risk-management program. Terms tailored to individual business needs and operational and cybersecurity risks will provide an organization the rights to enforce security requirements that will enhance supply-chain risk mitigation and shift certain liabilities in the event of a failure in the controls or breach of contract. However, these do not prevent a failure by a supplier or within the supply chain. These are just one of several defense-in-depth measures that enhance supply-chain risk-mitigation maturity for an organization.

Prior to developing terms for procurement agreements to address BESS supply-chain cybersecurity risks, the organization's standard terms and conditions used for all suppliers should be evaluated to determine what existing requirements support the objectives and whether any of these need to be enhanced for use with BESS product and service procurements. Examples of categories for typical general or standard terms and conditions can be defined as follows:

- **Basic physical, information, and cybersecurity controls.** General terms setting forth a high-level requirement to have a security program and follow it. These usually do not get into security-framework domain-specific details; instead, they merely set a simple obligation. These are not sufficient to protect the organization in the event of a cybersecurity or supply-chain failure.
- **Vendor Training Requirements.** Terms requiring vendors complete basic training, meet certification standards for any specialized skillsets, and comply with any requests to complete organizational training requirements (e.g., for entity-specific information restrictions and use of assets). Specific requirements may be warranted for security awareness and communications.
- **Vendor-Personnel Background Checks.** Terms setting forth minimum background-check standards for vendor employees and subcontractors. The entity may want to mandate background checks be conducted on vendor personnel with responsibilities that may impact the security of the procured BESS product or service.
- **Information-Sharing Restrictions.** Commonly included non-disclosure, information-protection, and data-destruction requirements may need to be expanded to ensure information access, use, management, destruction for data that presents additional risks to the BESS products and services.
- **Vendor Monitoring and Audit Provisions.** Obligations for vendors to conduct self-assessments and audits or to submit to monitoring and audit activities. Where supply-chain and security risks are potentially significant, these are typically included with specific periodicities and rights of the organization to request reports or specific data or even to conduct assessments and audits themselves.
- **Vendor Metrics.** Defined metrics specific to product performance or services. These may be important for certain BESS equipment. For example, it might be important to define terms relating to data integrity, operational performance, communications to meet new inverter-based requirements for distribution and bulk-power-grid reliability and security.
- **Compliance with Laws and Regulations.** These are standard for most contracts. Terms specifying an obligation to monitor for changes in law and other legal obligations, notify the organization, and update compliance are likely warranted for dynamic regulatory areas like supply-chain and cybersecurity.

5.2. Sample Procurement Agreement Terms

The sample provisions included below are specific to terms and conditions addressing potential cybersecurity risks within the BESS supply chain. These should be integrated and aligned to fit within existing broader procurement-agreement terms (e.g., entity master terms and conditions and other terms added to the specific vendor contract). Each customer should also review its entity specific supply-chain risk-management program to ensure any additional terms and concepts have been included. Sample defined terms are capitalized throughout and included in Appendix A: Sample Definitions.

Sample procurement-agreement definitions are included in Appendix A, Sample Procurement Agreement:

and Definitions. Please note disclaimer in Figure 12.

Not all terms will be needed for all vendors; not all requirements will need to be imposed at the same level of rigor for all vendors. For example, not all procurements will require a full-framework, documented cybersecurity program; rather, it may only be necessary to verify the existence of basic controls. A full SBOM may not be able to be obtained, but a term may be needed to ensure it is attempted and provided as soon as additional detail is available. The organization's procurement processes and any supplier risk-assessment controls may inform which terms will be used for specific procurements. Standard terms and conditions should always be reviewed before providing the procurement agreement for initial review to ensure they are tailored for the context of the specific supplier activities and commitments.


Disclaimer: This BESS Procurement Guide and these terms and conditions do not purport to provide legal advice. Counsel should be consulted to obtain advice and guidance for use within any agreement. 

Figure 12: Legal Disclaimer, BESS procurement guide Sample Procurement Agreement Terms.

5.3. General Terms

This [Agreement/Appendix] sets forth minimum cyber, physical, and supply chain security requirements that the [Contractor] must maintain for the term of this agreement. Any applicable [entity/organization service provider] processes supporting [Contractor] compliance to these terms will be provided to [Contractor] [describe means of transmittal or access for contractor].

5.4. General Product and Services Cyber and Supply Chain Security

[Contractor] shall have a documented cybersecurity program with defined controls that are implemented and maintained in accordance with a recognized Cybersecurity Standards Framework [if entity does not include in Definitions section, will need to define here]. Program controls shall include, but not be limited to the following domain elements and be designed in accordance with the Cybersecurity Standards Framework:

- **Notification of Security Event or Incident.** [Contractor] agrees to notify [Company] immediately upon discovery of a known or reasonably suspected Security Event or Incident. The notice shall include an initial written report containing the following information: (a) date of discovery and date of actual event/incident; (b) description of event/incident; (c) summary of impact to [Contractor] and whether any potential material impact has been identified; (d) summary of any impact to [Company]; (e) summary of causes; (f) summary of all immediate and planned mitigation measures to address the event/incident and prevent recurrence.

If the Security Event or Incident arises from [Contractor]-provided software, hardware, equipment, or services [Contractor] shall develop necessary remediation action to mitigate immediate and future harm to [Company] and cooperate with [Company] efforts to minimize harm to [Company].

Upon request, [Contractor] shall provide to [Company] written updates to the initial notification and report with any new or changed information or circumstances for any of the above-listed requested information categories. Such updates shall be provided within a reasonable period of time from discovery of the new or changed information or circumstances.

If the details of the issue, impact, or cause are not yet available, an initial notice shall be provided, followed by additional detail with required updates. [Company] shall have the right to request additional reports, details, and investigation information.

In the event [Contractor] is required by law or officially requested by law enforcement to withhold notification, [Contractor] will not be required to provide notification until such time as permitted. However, [Contractor] shall document the required notification information along with a summary of the justification for withholding and any formal documentation of law-enforcement requests to be provided to [Company] on request.

[Contractor] shall cooperate with [Company] to support all [Company] efforts to determine the extent and impact of any risks to [Company] resulting from the identified Security Event or Incident.

- **Incident Response.** [Contractor] shall develop and implement a Security Incident Response Plan in accordance with a recognized Cybersecurity Standards Framework, which shall include processes and controls to identify, assess, escalate, respond, report, remediate, and mitigate Security Incidents. [Contractor] shall, upon request, provide the [Contractor] Incident Response Plan for review. To the extent the Plan includes any proprietary or privileged information, [Contractor] shall have the right to redact such information.

[Contractor] will, at its sole cost and expense, assist [Company] with any [Company] investigation of, and response to, any identified Security Incident or Event, including disclosures to other parties, regulatory actions, legal actions, and other activities required pursuant to [Company] legal obligations or as otherwise required by law.

If a Security Incident results in the Disclosure of [Company] Information that results in required [Company] action including, but not limited to, notifications to customers, shareholders, current or former employees or contractors, law enforcement or any other notifications required by [Company] legal obligations or otherwise required by law, such notification shall be provided by [Company], except as required by law or where approved in writing by [Company]. [Contractor] will assist and cooperate with [Company] in its effort to meet any notification requirements. [Company] will have sole control over the timing and method of notifications.

- **Vulnerability Disclosure.** [Entity should consider to whom disclosure will be required and whether it will be limited to company or additional parties. This may be defined elsewhere and possibly here.] [Contractor] shall develop and implement processes to ensure the disclosure by [Contractor] of known Vulnerabilities and defects related to [Contractor] provided products and services under this [Agreement], including:
 - Prior to provision of procured product or service, [Contractor] shall submit a summary of publicly disclosed vulnerabilities and material defects in the product or services, including any available documentation, the potential impact, summary of any [Contractor] efforts to mitigate the vulnerabilities, any [Contractor] recommended corrective actions, compensating controls, mitigation recommendations and/or procedural workarounds.
 - For vulnerabilities or defects discovered at any time in the course of the provision of products or services under the Agreement, [Contractor] shall, within thirty (30) calendar days after such vulnerabilities and material defects become known to [Contractor], submit the report and information detailed in provision [above].
 - [Contractor] shall disclose the existence of all known methods for bypassing Authentication protocols and/or controls in the procured product or services, such as backdoors, and provide a written attestation that all such backdoors have been permanently remediated by [Contractor].
- **Hardware, Firmware, Software Authenticity.** Contractor shall establish, document, and implement risk-management practices for supply-chain security related to the delivery of hardware, software (including patches), and firmware provided under this [Agreement], in accordance with industry standards and until otherwise noted at end of sale, end of support, and/or end of life.

[Contractor] shall provide documentation on its chain-of-custody practices, inventory-management program (including the location and protection of spare parts), information-protection practices, integrity-management program for components provided by sub-tier suppliers, instructions on how to request replacement parts, and commitments to ensure that for [specified time] spare parts shall be made available by [Contractor]. [Contractor] shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

[Contractor] shall identify or provide [Company] with a method to identify the country (or countries) of origin of the procured [Contractor] product and its components (including country of manufacture (hardware) and country of build (software and firmware)). [Contractor] will identify the countries where the development, manufacturing, maintenance, and service for any [Contractor] products are provided. [Contractor] will notify [Company] of changes in the list of countries where product maintenance or other services are provided in support of the procured [Contractor] product. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

[Contractor] shall provide a software bill of materials (SBOM) and hardware bill of materials (HBOM) for any procured products provided under this [Agreement], consisting of a list of components and associated metadata for any components. For SBOMs, these shall include licensed products. If available SBOM or HBOM is incomplete due to circumstances out of the control of [Contractor], the SBOM or HBOM will be provided with a summary of any incomplete data and any measures in place to ensure updates are provided as soon as the missing information is available.

[Company] has the right to require inspection of [Contractor] [products] procured and supported under this [Agreement] for purposes of confirming, auditing, assessing the credibility of, and/or developing a SBOM and/or HBOM for any products procured or supported by services under this [Agreement]. [Company] may conduct the inspection or use a third-party vendor or agent of its choosing.

If, at any time, [Company] discovers a material inaccuracy or misrepresentation in the SBOM and/or HBOM associated with [Contractor] [products] procured and supported under this [Agreement] [Company] shall have the right to take any remediation measures [Company] deems, in its sole discretion, necessary, including and up to removal of the [assets].

- **Viruses and Malware.** In providing any products and services described in this [Agreement], including any third-party hardware, software (including open-source software), and firmware, [Contractor] shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses for any such products within [defined period] days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [defined period] days. If updates cannot be integrated, tested, and made available by [Contractor] within these time periods, [Contractor] shall provide recommended mitigations, methods of exploit detection, and/or workarounds within [defined period].

[Contractor] shall verify and provide documentation that procured products (including third-party products) have been appropriately updated and patched prior to supplying such product or service to [Company].

If [Contractor] provides software or patches to [Company], [Contractor] shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) 140-2, "Security Requirements for Cryptographic Modules," or similar standard information on the software and patches to enable [Company] to use the hash value to independently verify the integrity of the software and patches.

Upon request by [Company], and if such information is not confidential or [Contractor] Proprietary Information or otherwise protected by legal privilege, [Contractor] shall specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. When product features and delivery mechanisms allow, [Contractor] shall apply [requested standard] encryption technology to protect procured products throughout the delivery process.

Unless otherwise authorized and approved by [Company] in writing, products and services supplied by [Contractor] shall not require the use of any out-of-date, unsupported, or end-of-life versions of third-party components.

Prior to the delivery of any products and/or services to [Company] or any connection of electronic devices, assets, or equipment to [Company] assets or equipment, [Contractor] shall provide documentation establishing compliance by the [Contractor] to the implementation of a [Contractor] Vulnerability and Patch Management Program, set forth in the requirements in [reference Agreement paragraph] herein. [Refers to the Cyber Hygiene requirements below, if that term is not used, will need to integrate up here.]

[Contractor] will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to [Company]. To the extent [Contractor] is supplying third-party software or patches, [Contractor] will use reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any software or patches providing them to [Company] or installing them on [Company]'s networks and systems.

[Contractor] warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and [Contractor] will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality. To the extent [Contractor] is supplying third-party software or patches, [Contractor] will use reasonable efforts to ensure the third-party will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

When install files, scripts, firmware, or other [Contractor]-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an antivirus vendor, [Contractor] must provide or arrange for the provision of technical justification as to why the “false positive” hit took place to ensure their code’s supply chain has not been compromised.

If a virus or other malware is found to have been coded or otherwise introduced as a direct result of [Contractor]’s breach of its obligations under this [Agreement], [Contractor] shall, upon written request by [Company] and at its own cost, take all commercially reasonable action to eliminate the virus or other malware throughout [Company]’s networks and systems, and if the virus or other malware causes a loss of operational efficiency or any loss of data (i) where [Contractor] is obligated under this [Agreement] to back up such data, take all commercially reasonable steps necessary and provide all assistance required by [Company] and its affiliates, or (ii) where [Contractor] is not obligated under this [Agreement] to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

- **Data Integrity and Cryptographic Requirements.** [Contractor] shall document how the cryptographic system supporting the [Contractor]’s products and/or services procured under this [Agreement] protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to, the following: (i) the cryptographic methods (hash functions, symmetric-key algorithms, or asymmetric-key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]-256, Advanced Encryption Standard [AES]-128, Rivest-Shamir-Adleman and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented; (ii) the preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

[Contractor] will use only approved cryptographic methods, as defined in the FIPS 140-2 Standard when enabling encryption on its products.

As mutually agreed, [Contractor] shall provide or arrange for the provision of an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

[Contractor] shall ensure that (i) as mutually agreed, the system implementation includes the capability for configurable cryptoperiods (the lifespan of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of National Institute of Standards and Technology (NIST) 800-57, Part 1, as may be amended; (ii) as mutually agreed, the key-update method supports remote rekeying of all devices within [a negotiated time periods] as part of normal system operations; (iii) emergency rekeying of all devices can be performed remotely or on site within 30 days.

[Contractor] shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

- **[Contractor]** Access to **[Company]** systems.

[Contractor] shall coordinate with **[Company]** on all remote access to **[Company]**'s systems and networks, regardless of interactivity, and shall comply with any **[Company]** processes and controls for interactive remote access and system-to-system remote access, even for any access sessions requested by **[Company]**.

If **[Contractor]** directly, or through any of their affiliates, subcontractors, or service providers, connects to **[Company]**'s systems or networks, **[Contractor]** shall comply with all **[Company]** processes governing interactive remote access and system-to-system access. **[Contractor]** agrees to the following protective measures even where not formally defined in the **[Company]** remote access processes:

- [Contractor]** will not access and will not permit any other person or entity to access **[Company]**'s systems or networks without **[Company]**'s written authorization, and any such actual or attempted access will be consistent with any such written authorization.
- [Contractor]** shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.
- [Contractor]** shall ensure **[Contractor]** personnel do not use any virtual private network or other device to simultaneously connect machines on any **[Company]** system or network to any machines on any Contractor or third-party systems, without
 - Using only a remote access method consistent with **[Company]**'s remote-access control policies,
 - Providing **[Company]** with the full name of each individual who uses any such remote-access method and the phone number and email address at which the individual may be reached while using the remote access method, and
 - Ensuring that any computer used by **[Contractor]** personnel to remotely access any **[Company]** system or network will not simultaneously access the Internet or any other third-party system or network while logged on to **[Company]** systems or networks.

[Contractor] shall ensure **[Contractor]** personnel accessing **[Company]** networks are uniquely identified and that accounts are not shared between **[Contractor]** personnel.

5.5. Enterprise Cybersecurity and Supplier Cyber Hygiene Requirements

The following requirements are to ensure the Contractor has an enterprise cybersecurity program that aligns to a recognized Cybersecurity Standards Framework and is implemented within the organization and applied to all company assets.

- **Cybersecurity Program.** **[Contractor]** will have a documented cybersecurity policy which shall be consistent with industry standard practices (e.g., NIST Special Publication 800-53 (Rev. 4) as may be amended). **[Contractor]** will implement and comply with its established cybersecurity policy. Any changes to **[Contractor]**'s cybersecurity policy as applied to products and services provided to **[Company]** under this **[Agreement]** and any **[Company]** Information shall not decrease the protections afforded to **[Company]** or **[Company]** Information and any material changes shall be communicated to the **[Company]** in writing by **[Contractor]** prior to implementation.

[May prefer to include a provision that sets up the Cybersecurity Program with the policy using this language above and then the "implement" being "controls addressing each of the following:" then integrate the below sections as subsets to this section.]

- **Asset Identification and Management.** [Contractor] shall have processes for the development of an asset inventory that ensures [Contractor] ability to identify, prioritize and protect [high-risk], restricted, critical assets, including information/data, and continuously to evaluate the applicability of cybersecurity-program controls to all assets. The processes should include standards for asset classification to support the implementation of the risk-assessment and other controls to mitigate Security Incidents.
- **Risk-Assessment Processes.** [Contractor] shall have a process for identifying, prioritizing, and mitigating security risks to systems, hardware, firmware, software, and information/data.
- **Access Controls and Management.** [Contractor] shall implement controls defining security requirements for remote and onsite access to [Contractor] networks, systems, and/or information, including for high-risk, restricted, and critical assets. [Contractor] shall have defined processes for the review, approval and provisioning of access, for periodic review and verification of access, and timely removal of access, including a control for immediate removal where someone with access to [Contractor] networks, systems, and/or information are terminated for cause. [Entity may want to add a provision for access to Company systems and information that is not typically part of the cybersecurity-hygiene requirements for the Contractor, so it may need to be defined here or above.]
- **Authentication Requirements.** [Contractor] shall implement controls to monitor, identify, verify, and authenticate users accessing [Contractor] systems and information. These should include remote-access and enhanced-authentication controls such as multifactor authentication.
- **Configuration and Change Management.** [Contractor] shall implement controls to establish and maintain the configuration of [Contractor's] system Network Architecture(s) and Baseline(s), including hardware, software, firmware. This includes processes to ensure timely update when new assets are integrated or in the event of changes to/removal of existing assets.
- **Information Protection.** [Contractor] shall implement information-classification and protection procedures to ensure the identification, classification, protection, management, and destruction of confidential, restricted, classified and other protected data, as well as compliance to applicable privacy and information disclosure regulations.
- **Security Information and Event Management.** [Contractor] shall have defined protocols and use system tools to ensure the monitoring and timely identification of potential security threats and vulnerabilities such as commonly recognized security information and event management (SIEM) tools that collect, analyze, and support escalation and response to potential threats and Security Incidents. [Contractor] shall have a defined process for the timely initial analysis, escalation, review of identified potential threats and Security Incidents that includes guidance for prioritization and initiation of the Incident Response procedures.
- **Incident Response.** [Contractor] shall develop and implement a Security Incident Response Plan in accordance with a recognized Cybersecurity Standards Framework, which shall include processes and controls to identify, assess, escalate, respond, report, remediate, and mitigate Security Incidents.
- **Password Requirements.** [Contractor] shall implement policies defining minimum requirements for password complexity, periodic updates to user passwords, restrictions on reuse of passwords, failed-attempts lockout, and escalation rules.
- **Patch and Vulnerability Management.** [Contractor] shall implement a program for the monitoring and timely identification of issued patches, assessment processes to determine applicability and define implementation plans, minimum requirements for patching of [high-risk] assets, review, approval and exception processes for assessment determinations, guidelines for identifying, implementing and documenting mitigation measures where patches cannot be implemented within a reasonable period of time [Entity may want to consider defining this more specifically or expanding on the concept].

[Contractor] program shall include controls for remediation of newly reported zero-day vulnerabilities.

- **Security Assessments.** [Contractor] shall have processes to ensure defined periodic security assessments such as vulnerability assessments and penetration testing.
- **System Backup and Recovery.** [Contractor] shall ensure there are system redundancies and backups for all critical assets and data, periodic drills and testing of backups, a defined backup and recovery plan in the event of a cybersecurity incident, disaster, or other event that results in [downtime or system/asset failure].
- **Program Assessment and Audit.** [Contractor] shall define requirements for periodic self-assessment and third-party evaluation of Contractor's security program.
- **Training, Communications, and Awareness.** [Contractor] shall implement an enterprise training, communications, and awareness program to ensure all [Contractor] personnel have a general understanding of the security-program requirements and that [Contractor] personnel with controls accountability have the requisite experience and complete periodic training relevant to their defined cybersecurity-program role and responsibilities.

5.6. BESS Product- and Service-Related Security Terms

[Company] has the right to require inspection of [Contractor] [products] procured and supported under this [Agreement] for purposes of confirming, auditing, assessing the credibility of, and/or developing an SBOM and/or HBOM for any products procured or supported by services under this [Agreement]. [Company] may conduct the inspection or use a third-party vendor or agent of its choosing.

If, at any time, [Company] discovers a material inaccuracy or misrepresentation in the SBOM and/or HBOM associated with [Contractor] [products] procured and supported under this [Agreement], [Company] shall have the right to take any remediation measures [Company] deems, in its sole discretion, necessary, including and up to removal of the [products/equipment/assets].

6. MATURING BESS SUPPLY-CHAIN CYBERSECURITY: SUPPLIER MANAGEMENT AND COMPLIANCE CONTROLS

As a last key consideration in initial SCRM cybersecurity-process improvements, a review of vendor management processes should be completed to ensure the SCRM cybersecurity-process improvements are effectively integrated. Primary focus should be on:

- **Vendor Compliance to SCRM Requirements.** A control may need to be developed to monitor vendor compliance to SCRM contractual terms that were ultimately applied and included in the procurement agreement. Which controls and how they are applied should be commensurate to the risk, so including a data point with the inventory to inform monitoring and enforcement requirements would also be useful. For example, a high-risk vendor that provides equipment with a limited SBOM may warrant annual cybersecurity assessments that include a focus on specific requirements included in the original agreement.
- **Vendor Inventory Management.** The importance of a good inventory is discussed above in 3.2. The initial development will inform the improved SCRM processes and controls, but it will be equally important to maintain this inventory. This will require controls for internal monitoring for updates—e.g., inclusion of new vendors, changes or removals of vendors, changes in circumstances (e.g., Merger & Acquisition activity) for vendors or suppliers. Additionally, a specific process for identifying expiration of legacy agreements and/or other triggers that may allow for the application of the new program requirements should be considered to maximize opportunity to address issues with legacy assets.
- **Security Risk and Threat-Landscape Monitoring.** The procurement function should also set up a means for coordinating with any function that supports the monitoring, identification, assessment, and implementation of security alerts that may be applicable to product and services suppliers and critical data points for the SCRM program. For example, an presidential Executive Order or other critical alert issued identifying new products, manufacturers, or country-of-origin-related risks must be reviewed by procurement in coordination with Legal counsel to determine whether any of the existing vendor relationships, products, and/or services may be implicated, to assess required action, and to coordinate internally in the design of proper risk-mitigation measures that include the procurement activities.

7. CONCLUSION

As the prevalence of BESS, IBRs, and other related digital equipment continues to grow, so does organizations' reliance on a supply chain that is largely dominated by companies that design, operate, manufacture and/or assemble in foreign countries. Given the digital components of this equipment and its criticality for maintaining power system reliability, it is increasingly important to address the cyber supply chain risks for these devices. Mitigating cyber supply chain risks starts with a robust and intentional procurement process. An organization should take inventory of the vendors already in their ecosystem as part of the process to baseline risk. When new BESS, IBR, and related digital equipment is procured, specific guidance for RFPs can help create mutual understanding of expectations before vendors submit bids for project. After receiving RFPs, the vendor risk assessment methodology described in this guide can help organizations assess and quantify risks associated with each vendor as well as identify ways to mitigate known risks. The sample procurement language provided in this guide can protect organizations and provide legal mechanisms to enforce the risk mitigation measures and responsibilities for the vendor.

8. REFERENCES

1. NREL Fall Solar Industry Update FY23," 2024. [Online]. Available: <https://www.nrel.gov/docs/fy24osti/88026.pdf>. [Accessed: April 24, 2024]
2. NERC. n.d. "Supply Chain Risk Mitigation Program." North American Electric Reliability Corporation (NERC), Atlanta, GA. Accessed September 9, 2024. <https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx>.
3. M.. Papaphillippou, K. Moulinos, and M. Theocharidou. 2023. "Good Practices for Supply Chain Cybersecurity." European Union Agency for Cybersecurity (ENISA), Athens, Greece. <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>.
4. DOE. n.d. "Supply Chain Cybersecurity Principles." U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response. <https://www.energy.gov/sites/default/files/2024-06/DOE%20Supply%20Chain%20Cyber%20Principles%20June%202024.pdf>.
5. W. Grant. 2024. "How Chinese firms are using Mexico as a backdoor to the US." BBC, London, United Kingdom. <https://www.bbc.com/news/business-68825118>.
6. DOE. 2022. "Solar Photovoltaics: Supply Chain Deep Dive Assessment, U.S. Department of Energy Response to Executive Order 14017, 'America's Supply Chains.'" U.S. Department of Energy. <https://www.energy.gov/sites/default/files/2022-02/Solar%20Energy%20Supply%20Chain%20Report%20-%20Final.pdf>.
7. NIST. n.d. "Glossary." National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), Updated August 19, 2024. <https://csrc.nist.gov/glossary/>.
8. NERC. 2024. "Glossary of Terms Used in NERC Reliability Standards." North American Electric Reliability Corporation (NERC), Updated August 28, 2024. https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.
9. NICCS. n.d. "Vocabulary: Explore Terms: A Glossary of Common Cybersecurity Words and Phrases." National Initiative for Cybersecurity Careers and Studies (NICCS). <https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary>.
10. FERC. 2023. "Critical Energy/Electric Infrastructure Information (CEII)." Federal Energy Regulatory Commission (FERC), Accessed September 9, 2024. <https://www.ferc.gov/ceii>.
11. Cybersecurity and Infrastructure Security Agency (CISA). 2023. "Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management." CISA. Accessed September 9, 2024. <https://www.cisa.gov/sites/default/files/2023-09/A%20Hardware%20Bill%20of%20Materials%20Framework%20for%20Supply%20Chain%20Risk%20Management%20%28508%29.pdf>.
12. CISA. n.d. "Software Bill of Materials (SBOM)." Cybersecurity and Infrastructure Security Agency (CISA). Accessed September 9, 2024. <https://www.cisa.gov/sbom>.
13. SCADA. n.d. "What is SCADA?" SCADA International. Accessed September 9, 2024. <https://scada-international.com/what-is-scada/>.

Appendix A

Sample Procurement Agreement: Contract Definitions

These sample contract definitions are used throughout the Sample Procurement Agreement Terms set forth in Section 5 of this guide. Entities using any of the sample terms in Section 5 above, and these sample definitions should review carefully to ensure alignment. Sources used for these term definitions include NIST [7], NERC [8], and CISA [9]. Source reference are included in brackets at the end of most defined terms so the entity using them can verify the definition is current and determine whether to include the reference in the specific agreement.

Definitions

The sample definitions below are specific to the sample procurement agreement terms for BESS systems and cybersecurity risks provided above in Section 5 of this guide. General definitions should be added, including terms to define confidential, restricted and other protected data that may be applicable and of interest for inclusion by the specific entity or to a specific vendor.

Access Control. The process of granting or denying specific requests to: i) obtain and use information or related systems or services or ii) enter specific physical facilities. [NIST]

Antispyware Software. A program that specializes in detecting both malware and non-malware forms of spyware. [NIST]

Antivirus Software. A program designed to detect many forms of malware (e.g., viruses and spyware) and prevent them from infecting computers. It may also cleanse already-infected computers. [NIST]

Authentication. Verifying the identity of a user, process, or system, often as a prerequisite to allowing access to resources in an information system. [NIST]

Baseline. Hardware, software, and relevant documentation for an information system at a given point in time. [NIST]

Baseline or System Configuration. A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. [NIST]

A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change-control procedures. [NIST]

Battery-Management System (BMS). A battery-management system is an electronic control unit that regulates and monitors the operation of a battery during charge and discharge. In addition, the battery-management system is responsible for connecting with other electronic units and exchanging the necessary data about battery parameters. The voltage, capacity, temperature, power consumption, state of charge and health, charging cycle, and other characteristics of the battery are controlled and monitored by the battery-management system.

BES (Bulk Electric System). Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher (subject to inclusions and exclusions). This does not include facilities used in the local distribution of electric energy. [NERC Glossary + added detail in parentheses]

BES Cyber Asset. A Cyber Asset that, if rendered unavailable, degraded, or misused, would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. [NERC glossary]

BES Cyber Security Information (BCSI). Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual Internet Protocol (IP) addresses without context, Encapsulating-Security-Payload (ESP) names, or policy statements. [NERC Glossary]

Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber systems, physical access control systems, and electronic access control or monitoring systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution, collections of network addresses, and network topology of the BES Cyber System. [NERC glossary]

BES Cyber System. One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity. [NERC glossary]

CEII (Critical Energy Infrastructure Information). Information related to or proposed to critical electric infrastructure, generated by or provided to [FERC] or another federal agency other than classified national-security information, and that is designated as critical electric-infrastructure information by [FERC] or the Secretary of the Department of Energy pursuant to Section 215A(d) of the Federal Power Act.

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

- Relates details about the production, generation, transmission, or distribution of energy
- Could be useful to a person planning an attack on critical infrastructure
- Is exempt from mandatory disclosure under the Freedom of Information Act
- Gives strategic information beyond the location of the critical infrastructure.

Critical Energy/Electric Infrastructure. A system or asset of the bulk-power system, (physical or virtual) the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters. [FERC (10)]

Compensating Control. A management, operational, and/or technical control (i.e., a safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. [NIST]

Contractor or Vendor or Supplier. A person or company that sells a product or service.

Critical Component. A component which is or contains information and/or communications technology [. . .], including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission-critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system. [NIST]

Cryptographic Modules. The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within a cryptographic boundary. [NIST]

Cyber Asset. Anything that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). [NIST]

Cyber Event. Any observable occurrence in a network or system. [NIST]

Cyber Incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable-use policies. [NIST]

Cybersecurity Standards Frameworks. A recognized set of cybersecurity standards that provide comprehensive guidance and best practices for organizations to follow to improve information security and cybersecurity-risk management. Examples include the NIST Cybersecurity Framework (NIST CSF), the Department of Energy (DOE) C2M2 Cybersecurity Maturity Model, the Center for Internet Security (CIS) Critical Security Controls Framework, International Standards Organization/International Electrotechnical Commission Standards (e.g., ISO 27001, “Information Security Management Systems”).

Data Breach. An incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit-card numbers, personal health information, customer data, company trade secrets, or matters of national security. [NIST]

Element. A statement about an Information Security Continuous Monitoring (ISCM) concept that is true for a well-implemented ISCM program. [NIST]

Electronic Security Perimeter. The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled. [NERC]

Encryption. The transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. [NIST]

Firewall. A device or program that restricts data-communication traffic to or from a network and thus protects that network’s system resources against threats from another network. [NIST]

Firmware. Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that the programs and data cannot be dynamically written or modified during execution of the programs. [NIST]

HBOM (Hardware Bill of Materials). The HBOM Framework for Supply Chain Risk Management product includes a consistent naming methodology for attributes of components, a format for identifying and providing information about the different types of components, and guidance of what HBOM information is appropriate, depending on the purpose for which the HBOM will be used. [CISA (11)]

Industrial Control System. An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial-control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. [NIST]

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display,

switching, interchange, transmission, or reception of data or information by [Company]. For purposes of the preceding sentence, equipment is used by [Company] if the equipment is used by the [Company] directly or is used by a contractor under a contract with the [Company] which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [NIST is the original source. Edited for use by Company.]

Intrusion Detection System (IDS). A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner. [NIST]

Least-Privileged. A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks. [NIST]

Malicious Code. Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. (CISA)

Malware. A computer program that is covertly placed onto a computer or electronic device with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems. Common types of malware include viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware. [NIST]

Network. An information system implemented with a collection of interconnected components such as computers, routers, hubs, cabling, and telecommunications controllers. [NIST]

Network Architecture. The logical and structural layout of a network, consisting of signal-transmission equipment, software and communication protocols, and (wired or wireless) infrastructure, transmission of data, and connectivity between components.

Operational Technology (OT). Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial-control systems, building-management systems, fire-control systems, and physical-access-control mechanisms. [NIST]

Packet. The logical unit of network communications produced by the transport layer. [NIST]

Personnel. Employees, contractors and other personnel providing services or support to the organization. *(This should be defined as part of entity general terms and conditions.)*

Physical Security Perimeter. The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled [NERC]

Power Conversion System (PCS). A device that converts electric energy from one form to another for storage or release of the energy in or from the battery. In order to obtain energy stored in an Energy Storage System (ESS), which is emerging as a solution to the energy shortage, a PCS converts the energy to the form required by the end user.

Protocol. Rules followed when transmitting and receiving or exchanging information.

Remote Access. Access to an organization’s information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). [NIST]

SBOM (Software Bill of Materials). A key building block in software security and software supply-chain risk management,. An SBOM is a nested inventory, a list of ingredients that make up software components. While not a brand-new concept, the ideas and implementation have advanced since 2018

through a number of collaborative community effort, including National Telecommunications and Information Administration's (NTIA) multistakeholder process. [CISA (12)]

Security Controls. Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [NIST]

Security Incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, procedures and/or acceptable-use policies. [NIST]

Site Controllers. The entity that coordinates control activities of the power-conditioning system to deliver active and reactive power to the load and provides the interface for a BESS operator to manually operate the BESS. The controller also monitors all BESS systems, including the fire-detection and suppression system and signals alarms through the SCADA interfaces.

Spyware. Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge. [NIST]

Security Program. Formal document that provides an overview of the security requirements for an organization-wide information-security program and describes the program-management controls and common controls in place or planned for meeting those requirements. [NIST]

Supervisory Control and Data Acquisition (SCADA). Systems used for controlling, monitoring, and analyzing industrial devices and processes. The system consists of both software and hardware components and enables remote and onsite gathering of data from industrial equipment. [SCADA International (13)]

Supply Chain. The network of all the individuals, organizations, resources, activities, and technology involved in the creation and sale of a product. The supply chain encompasses everything from the delivery of source materials from the supplier to the manufacturer through to its eventual delivery to the end user.

System Security. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [NIST]

Virus. A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. [NIST]

Vulnerability. A weakness in a system, application, or network that is subject to exploitation or misuse. [NIST]

Vulnerability Exploitability eXchange (VEX). A document type that is a form of a security advisory to indicate whether a product or products are affected by a known vulnerability or vulnerabilities. [CISA]

Vulnerability Management. A capability that identifies vulnerabilities on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network. [NIST]

Whitelist. An approved list or register of entities provided a particular privilege, service, mobility, access, or recognition. [NIST]

Zero-Day Exploit. An attack on a previously unknown hardware, firmware, or software vulnerability.
[NIST]